La protection des données à caractère personnel en droit communautaire

Boulanger, Marie-Helene; Léonard, Thierry; Louveaux, Sophie; Moreau, Damien; de Terwangne , Cécile; Poullet, Yves

Published in:
Telecommunications and Broadcasting Networks under EC Law : the Protection Afforded to Consumers and Undertakings in the Information Society

Publication date:
2000

Document Version
le PDF de l'éditeur

La protection des données à caractère personnel en droit communautaire[1]

Marie-Hélène Boulanger
Cécile de Terwangne
Thierry Léonard, Sophie Louveaux
Damien Moreau, Yves Poullet

Table des matières

1 Le présent article ne présente que l'opinion personnelle de ses auteurs.

A. Le contexte général

1. Le 24 octobre 1995, la Communauté européenne s'est dotée d'une directive générale concernant la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données[2].

Ce texte est l'aboutissement d'un long processus de réflexion et de recherche de consensus entre les différents États membres. C'est que la plupart de ceux-ci, conformément aux obligations contractées au sein du Conseil de l'Europe par la signature de la Convention n° 108[3], disposaient déjà d'une législation nationale ayant un objet similaire.

Si les principes de base de la protection sont analogues, les législations nationales présentent à l'heure actuelle de larges divergences susceptibles de freiner la libre circulation des informations dans le grand marché européen. En outre, l'internationalisation croissante des flux d'informations forçait une réflexion quant aux transferts de données vers les pays tiers[4]. Il fallait enfin tenter de mettre à jour ces législations en tenant compte des leçons tirées de nombreuses années d'application de la Convention n° 108.

2. Cette convention n'est, du reste, plus aujourd'hui le seul instrument international régissant tout ou partie de la protection des données à caractère personnel en Europe. L'Union européenne elle-même a adopté, ou est en passe de le faire, divers textes protecteurs dans le cadre soit de sa politique économique (la future directive RNIS[5], le règlement statistique[6], etc.) soit du troisième pilier – coopération dans les domaines de la justice et des affaires intérieures – (Convention Europol[7], future Convention Eurodac[8], etc.). D'autres textes sont issus de sources plus diverses : les nombreuses recommandations sectorielles du Conseil de l'Europe[9] mais aussi les dispositions de la Convention européenne des droits de l'homme susceptibles de s'appliquer[10], les lignes directrices de l'O.C.D.E.[11], la Convention d'Application de Schengen[12], etc.

L'existence de cette multiplicité de textes, parfois juridiquement contraignants, ne sera pas sans poser des problèmes aigus de légistique aux États membres qui doivent conformer à la directive leur législation nationale pour le 24 octobre 1998[13] tout en évitant d'enfreindre les dispositions issues d'autres instruments.

3. La filiation entre la directive et les textes issus du Conseil de l'Europe est évidente et explicite. Le considérant 10 de la directive indique ainsi que « l'objet des législations nationales relatives au traitement de données à caractère personnel est d'assurer le respect des droits et le butés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 C.E.D.H. et dans les principes généraux de droit communautaire ». Le considérant 11 énonce, quant à lui, que « les principes de protection des droits et libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la Convention du 28 janvier 1981 du Conseil de l'Europe ».

Outre des dispositions largement analogues, la similarité entre la directive et la Convention n° 108 se marque par la poursuite de deux objectifs apparemment identiques, à savoir, d'une part, la protection des libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard des traitements de données à caractère personnel[14] et, d'autre part, la libre circulation des données[15].

2 Directive 95/46/C.E. du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, J.O.C.E., n° L 281/31, du 23 novembre 1995 (ci-après dénommée « la directive »).

3 Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981, Série des traités européens, n° 108 (ci-après « la Convention n° 108 »). En principe, cette convention est dépourvue d'effets directs dans l'ordre juridique interne (voy. notamment point 20 du *Rapport explicatif de la Convention,* Conseil de l'Europe, Strasbourg, 1981). Toutefois, certains pays, comme la France, ont reconnu un tel effet à certains de ses articles.

4 La Convention n° 108 ne contient aucune disposition à cet égard.

5 Proposition de directive du Parlement européenne et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de service (RNIS) et des réseaux mobiles numériques, J.O.C.E., n° C 315, du 24 octobre 1996.

6 Règlement n 322/97 du Conseil, du 17 février, relatif à la statistique communautaire, J.O.C.E., n° L 52/1, du 22 février 1997.

7 Convention basée sur l'article K 3 du traité sur l'Union européenne portant création d'un office européen de police (convention Europol) J.O.C.E., n° C 316/2, du 27 novembre 1995.

8 Projet de Convention Eurodac, pour la collection, le stockage, l'échange et la comparaison des empreintes digitales des demandeurs d'asile.

9 Recommandations pour la protection des données utilisées à des fins de marketing (R (85) 20 du 25 octobre 1985), de sécurité sociale (R (86)1 du 23 janvier 1986), dans le secteur de la police (R (87) 15 du 15 septembre 1987, à des fins d'emploi. (R (89) 2 du 18 janvier 1989), à des fins de paiement (R (90) 19 du 13 septembre 1990), sur la communication à des tierces personnes des données à caractère personnel détenues par des organismes publics (R (91) 10 du 9 septembre 1991), relative à l'utilisation de l'ADN dans le cadre de la justice pénale (R (92) 1 du 10 février 1992), dans le domaine des services de télécommunications. (R (95) 4 du 7 février 1995); pour la protection des données médicales (R (97) 5 du 14 février 1997).
Certains textes plus anciens dans les domaines des assurances et de la recherche scientifique et statistique sont actuellement réexaminés. On peut encore citer la recommandation R (95) 11 du 11 septembre 1995 relative à la sélection, au traitement, à la présentation et à l'archivage des décisions judiciaires. Ces recommandations ne lient que moralement les États signataires.

10 Principalement l'article 8 (protection de la vie privée et familiale) et l'article 10 (liberté d'expression) de la Convention européenne des droits de l'homme (ci-après C.E.D.H.). Pour une analyse de l'article 8 C.E.D.H., voy. *C. Russo, in L. E. Pettiti, E. Decaux* et *P. H. Imbert,* La Convention européenne des droits de l'homme, Paris, Economica, 1995, p. 305 et ss; *E. Coussirat-Coustere,* idem. Pour une analyse récente de la jurisprudence relative à l'article 8, voy. *R. Ergec,* « Examen », R.C.J.B., 1995, p. 341 et *P. Lambert,* « Examen », J. T., 1996, p. 36 et s. Pour une jurisprudence appliquant l'article 8 C.E.D.H. à la protection des données voy. Cour eur. D. H., arrêt *Leander* du 26 mars 1987, série A, n° 116, § 48. Voy. aussi Req. n° 8334/78, X c. Autriche, Req. n° 1307/ 61, X c. République fédérale d'Allemagne et Req. n° 8170/78, citées par *P. Kayser,* La protection de la vie privée par le droit, Paris, Economica, 1995, p. 30. Voy. aussi Cour eur. D. H., arrêt *Klass,* du 6 septembre 1978, série A, n° 28; Cour eur. D. H., arrêt *Malone* du 2 août 1984, série A, n° 82; Cour eur. D.H., arrêt *Kruslin* du 24 avril 1990, série A, n° 176; Cour eur. D. H., arrêt *Huvig* du 24 avril 1990, série A, n° 176-B.

11 Lignes directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, Paris, O.C.D.E., 1981. Ce texte n'est que moralement contraignant.

12 Convention d'application de l'Accord de Schengen du 14 juin 1985.

13 Article 32, § 1, de la directive.

14 Cfr l'article ler de la Convention n° 108: « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamnent de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (protection des données) » et l'article 1 § 1 de la directive : « Les États membres assurent (. . .) la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard des traitements de données à caractère personnel ».

15 Voy. ci-dessous, pt. 6.

On pourrait bien sûr s'étonner d'une telle convergence. Ces textes sont en effet issus d'organisations internationales dont les buts premiers paraissent *a priori* aux antipodes les uns des autres : la protection des droits de l'homme et libertés fondamentales pour le Conseil de l'Europe, la réalisation d'un marché unique et la promotion de grandes libertés économiques pour l'Union européenne.

4. En réalité, le but véritable de la directive est d'éviter que la libre circulation de l'information entre États membres, liberté par essence économique, soit excessivement limitée – au surplus de manière différente au sein de chaque État – au nom de droits et libertés de la personne humaine. Dans la mesure où l'objectif premier de l'Union européenne[16] est la création d'un marché sans frontières internes, assurant la libre circulation des marchandises, personnes, services et capitaux, la libre circulation des données apparaît comme une condition indispensable de la création effective de ce marché[17]. Cette libre circulation exige qu'une protection des droits fondamentaux des personnes concernées par ces données soit assurée sinon de manière uniforme[18], du moins de façon équivalente dans les divers États membres, étant entendu qu'elle s'opère, selon les déclarations des considérants, à un niveau élevé[19].

5. On peut prévoir qu'à l'avenir, les législations nationales de protection des données deviendront, plus que jamais, le terrain d'une confrontation incessante entre, d'une part, les intérêts économiques et commerciaux de responsables de traitements qui n'auront de cesse de légitimer leurs traitements sur les grandes libertés économiques fondant l'Union européenne, et plus précisément sur l'« équilibre » consacré par les dispositions de la directive commentée, et d'autre part, les intérêts de la personne concernée par les données qui mettra en avant les droits et libertés fondamentales qui lui sont reconnus au sein de chaque État membre sur la base des conventions et autres instruments issus du Conseil de l'Europe. Les oppositions pourront d'ailleurs surgir lors d'applications non spécifiques à la libre circulation de l'information, mais par exemple à la liberté de concurrence[20] ou d'établissement.

C'est d'autant plus vrai que les protagonistes disposeront dans l'avenir de voies juridictionnelles différentes afin de tenter de résoudre les probables conflits. Les responsables des traitements préféreront certainement utiliser la voie des procédures introduites devant la Cour européenne de Luxembourg. Les personnes concernées opteront plutôt pour les procédures propres à la Convention européenne des droits de l'homme devant la Cour de Strasbourg. Même si l'on peut s'attendre à des rapprochements entre

16 Article 7 du Traité de l'Union européenne 7 février 1992, J.O.C.E., 1992, C 231, du 29 juillet 1992.

17 Voy. le considérant 3 de la directive. La Convention n° 108 poursuit le même objectif de libre circulation des données. C'est toutefois au nom de l'article 10 de la C.E.D.H. (liberté d'expression) que cet objectif doit être réalisé. Le rapport explicatif est très éclairant à cet égard: « Le ».

18 Il s'agit, dira-t-on, conformément au Traité européen de rapprocher les législations.

19 Le considérant 11 de la directive déclare que la directive « amplifie » les principes de la Convention n° 108.

20 Des divergences de réglementations nationales relatives aux données sensibles permises – on le verra – par la directive commentée, pourraient ainsi entraîner des distorsions de concurrence entre des entreprises concurrentes opérant à partir de territoires plus « laxistes ».

l'Union européenne et le Conseil de l'Europe[21], les différences de fondement de l'intervention des organes conjointement compétents risquent de déboucher sur des solutions difficilement conciliables.

Ce tiraillement risque encore d'être exacerbé dès lors qu'une marge de manouvre appréciable est laissée à chaque État membre dans la mise en vigueur des dispositions protectrices de la directive.

6. L'article 1, *b,* de la directive énonce que « les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre les États membres pour des raisons relatives à la protection assurée en vertu du § 1 »[22].

La première partie du considérant 9 précise à cet égard que « du fait de la protection équivalente résultant du rapprochement des législations nationales, les États membres ne pourront plus faire obstacle à la libre circulation entre eux des données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes notamment du droit à la vie privée »[23].

L'équivalence de protection décrétée par la directive n'abolit pas toute disparité entre législations nationales. Même si le degré de précision de la directive aurait pu le laisser penser, le considérant 9 atténue fortement ce qui, cependant, aurait dû constituer la conséquence logique de sa prémisse. Il affirme en effet que « les États membres disposeront d'une marge de manœuvre qui, dans le contexte de la mise en œuvre de la directive, pourra être utilisée par les partenaires économiques et sociaux ; qu'ils pourront donc préciser, dans leur législation nationale, les conditions générales du traitement des données ; que ce faisant, les États membres s'efforceront d'améliorer la protection assurée actuellement par leur législation ; que dans les limites de cette marge de manœuvre et conformément au droit communautaire, des disparités pourront se produire dans la mise en œuvre de la directive »[24].

7. Certaines dispositions de la directive reconnaissent explicitement la marge de manœuvre. En particulier à propos des flux intraeuropéens, le responsable établi sur plusieurs territoires veillera, selon l'article 4, à assurer le « respect par chacun des établissements des obligations prévues par le droit national applicable ». A propos des flux vers les pays tiers, selon l'article 25, c'est d'abord au regard des dispositions nationales prises en application des autres dispositions de la directive que s'opérera l'examen des flux. Plus fondamentalement, c'est à propos des principes fondamentaux de la protection des données que le considérant 22 souligne que « les États membres préciseront

21 Entre le Conseil de l'Union européenne et le Comité juridique de protection des données du Conseil de l'Europe, il existe un certain rapprochement, d'une part, via la coordination des textes – c'est ainsi que la conformité du texte de la recommandation R(97) 5 sur la protection des données médicales avec la directive a été examinée préalablement à son adoption –, d'autre part via des négociations en vue de l'adhésion de la Communauté européenne à la Convention n° 108 (voy. la recommandation de décision du Conseil de l'Union européenne relative à l'ouverture de négociations en vue de l'adhésion des Communautés européennes à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données). Dans un document de travail du 17 avril 1997 relatif à cette question, la Commission européenne estime que l'adhésion de la Communauté à la Convention n° 108 aurait pour conséquence d'intégrer celle-ci dans l'ordre juridique communautaire et ceci à un niveau normatif supérieur à la directive. Cette adhésion donnerait cependant compétence à la Cour de justice des Communautés européennes pour connaître du respect de la Convention n° 108. La jurisprudence de la Cour de justice des Communautés européennes considère que l'article 8 de la Convention européenne des droits de l'homme, voy. C.J.C.E., 5 octobre 1994, X c. Commission, C 404/92 P, Rev. trim. dr. h., 1995, p. 98, note (*O. de Schutter*).

22 L'article 12, § 2, de la Convention n° 108 stipule qu'« une ».

23 De manière similaire, le paragraphe 20 du Rapport explicatif de la Convention n° 108 précise qu'« en ».

24 L'article 12, §3, a, de la Convention n° 108 donne également aux États signataires une certaine marge de manœuvre dans la mesure où il les autorise à prévoir une réglementation spécifique pour certaines catégories de données pour autant que l'autre partie n'apporte pas un niveau de protection équivalent à celles-ci.

dans leur législation ou lors de leur mise en œuvre des dispositions prises en application de la présente directive les conditions générales dans lesquelles le traitement de données est licite ; qu'en particulier, l'article 5, en liaison avec les articles 7 et 8, permet aux États membres de prévoir, indépendamment des règles générales, des conditions particulières pour les traitements de données dans des secteurs spécifiques ».

Nombreuses sont du reste les dispositions explicites du texte où la plus grande liberté d'interprétation est laissée aux États membres même si elles visent parfois des éléments essentiels de la protection :

- la nécessité de l'exécution d'une mission d'intérêt public (art. 7, e), de nature à légitimer certains traitements, pourra être soumise à un contrôle particulier de l'autorité de contrôle ou exiger un fondement légal, selon les principes constitutionnels de chaque pays ;
- à propos des données sensibles, l'article 8, § 2, *a,* autorise chaque État à limiter la portée du consentement de la personne concernée dans tous ou certains traitements portant sur de telles données, l'article 8, § 2, *b,* laisse à la législation nationale le soin de définir les traitements de données sensibles justifiés par le respect des obligations et droits nés des législations de droit du travail ainsi que les garanties adéquates entourant de tels traitements, l'article 8, § 4, permet à l'État de légitimer pour des motifs d'intérêt public comportant des traitements de données sensibles au-delà des cas prévus par le reste de l'article 8, enfin, l'article 8, § 7, laisse aux États membres le soin de régler la question des numéros d'identification, nationaux ou de portée générale ;
- l'article 9 confère aux États membres le soin de réglementer le secteur de la presse ;
- l'article 11 relatif à l'information des personnes concernées lorsque les données n'ont pas été collectées auprès de la personne concernée contient une alternative importante quant au moment de cette information et des possibilités de dérogations importantes, dont chaque État pourra se prévaloir ou non ;
- l'article 13 permet à chaque État de limiter certains droits prévus par la directive lorsqu'une limitation est nécessaire pour la sauvegarde d'intérêts publics importants, voire de la protection de la personne concernée ou des droits et libertés d'autrui[25] ;
- le droit d'opposition prévu à l'article 14 peut être limité par le droit national et l'article 15 autorise pareillement une législation nationale à légitimer les décisions individuelles fondées exclusivement sur un traitement automatisé ;
- dans le domaine des obligations administratives de notification à l'autorité de contrôle ou de contrôle préalable, les articles 18, 19, 20 et 21 laissent aux États membres de nombreuses latitudes qui peuvent conduire à des régimes profondément différents qui pourraient influer sur le choix des entreprises à localiser leurs traitements dans tel ou tel État ;
- l'article 24 laisse aux États membres le soin de définir les mesures d'application de la directive et en particulier les sanctions de la violation des dispositions prises en application de celle-ci.

8. Si les auteurs de la directive paraissent avoir été conscients de l'importante marge de manœuvre laissée aux États membres nonobstant le rapprochement des législations opéré par la directive, ils ont en même temps mis en place les instruments d'une nécessaire mais progressive convergence.

25 L'article 9, a et b, de la Convention n° 108 contient une disposition identique, à savoir qu'il « est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :
a. à la protection de la sécurité de l'État, à la sûreté de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;
b. à la protection de la personne concernée et des droits et libertés d'autrui ».

On peut ainsi noter à ce propos que :

- en matière de flux transfrontières vers les pays tiers, la politique nationale trouve ses limites dans l'obligation d'informer la Commission tant des autorisations que des refus, ce qui permet à la Commission, avec l'aide du Comité des représentants des États membres de définir une politique commune en la matière ;
- la constatation de « divergences susceptibles de porter atteinte à l'équivalence des niveaux de protection » fait l'objet d'un suivi par le « Groupe de protection des personnes », composé de représentants des autorités de contrôle. Ce groupe peut également proposer des interprétations communes du texte de la directive ;
- un mécanisme puissant de convergence est constitué par la mise sur pied de codes de conduite communautaires qui échappent à l'examen des autorités nationales de protection des données ;
- la prohibition pour des raisons relatives à la protection des données, des restrictions ou interdictions des flux de données à l'intérieur de l'Union européenne, représente une incitation forte pour les pays à ne pas exiger des protections nationales sensiblement plus fortes, protections dont l'efficacité pourrait facilement être détournées par un flux interne à l'Union européenne.

Ainsi, si on doit parler de liberté relative des États membres, cette liberté apparaît surveillée, à défaut d'être contrôlée.

9. Le présent commentaire suivra largement le plan des dispositions de la directive[26], même si le champ d'application territorial de celle-ci sera étudié, pour des raisons de meilleure compréhension, dans la partie relative aux flux transfrontières de données.

On s'attachera dans un premier temps aux définitions (2), ce qui permettra de mesurer au mieux le champ d'application matériel de la directive (3). On s'attardera ensuite sur les lignes directrices de la protection (4) et sur l'étude des régimes spécifiques à certaines catégories de traitements (5). Les droits de la personne concernée retiendront alors l'attention ainsi que certaines obligations spécifiques du responsable du traitement (6). Le régime spécifique des flux transfrontières de données fera l'objet d'une large analyse en distinguant les flux intracommunautaires, en ce compris le champ d'application territorial, et ceux poursuivis vers des pays tiers (7). On terminera par un bref commentaire des dispositions relatives à l'utilisation des code de conduite (8), à l'institution d'organes de contrôle et d'interprétation (9) et aux responsabilités (10).

26 Bien que procédant d'une logique similaire, la structure de la directive n'est pas totalement identique à celle de la Convention n° 108 : elle y ajoute de nouveaux chapitres ; elle regroupe certaines dispositions de manière différente. L'objet des chapitres un et deux de la directive et de la Convention n° 108 est identique. Le chapitre trois de la directive porte sur la responsabilité, les recours et les sanctions, alors que la Convention n° 108 ne traite pas ces questions dans un chapitre spécifique, mais les aborde dans le chapitre deux, qui contient l'ensemble des principes à la base de la protection. Le chapitre quatre de la directive, intitulé, à l'instar du chapitre quatre de la Convention n° 108 « Flux transfrontières de données » a en réalité un objet différent. Le chapitre quatre de la Convention n° 108 envisage la question des flux transfrontières entre pays liés par cette Convention, tandis que le chapitre quatre de la directive règle les flux transfrontières vers les États non liés par la directive. Le chapitre cinq de la directive relatif aux codes de conduite ne trouve pas d'équivalent dans la Convention n° 108. Enfin, le chapitre six de la directive concernant les autorités nationales de contrôle et le groupe communautaire de protection des données regroupe des dispositions contenues dans les chapitres deux et quatre de la Convention n° 108.

B. Définitions

10. Les réglementations relatives à la protection des données doivent être, autant que possible, indépendantes des évolutions incessantes des technologies de l'information. C'est pourquoi – et la directive commentée ne fait pas exception – leur champ d'application matériel est déterminé au moyen de concepts juridiques abstraits prédéfinis (traitements, données à caractère personnel, etc.). Ces définitions permettent l'insertion des dernières évolutions technologiques dans le champ des réglementations même si le contenu des règles doit, selon les cas, être adapté.

C'est ainsi que la directive européenne s'appliquera, non seulement aux banques de données classiques contenant de l'information personnelle, mais également à des techniques plus évoluées de collectes d'informations (systèmes d'enregistrements d'images numérisées, call centers automatisés, etc.) ou de transmissions d'informations (réseaux mondiaux du type d'Internet, systèmes E.D.I. etc.).

En outre, afin de déterminer au mieux les responsabilités quant aux règles de comportement édictées, d'autres définitions sont également arrêtées : responsable du traitement, sous-traitant, etc.

I. Les données à caractère personnel

11. Selon l'article 2, a, de la directive, est considérée comme donnée à caractère personnel, « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement ; notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[27].

La notion d'information n'est pas définie. Dès lors, elle n'est soumise à aucune exigence de forme particulière. Une information écrite, chiffrée, mais celle également présente dans une image ou un son sont constitutives de données[28].

27 Dans la Convention n° 108, la donnée à caractère personnel signifie « toute ».

28 Voy. le considérant 14 de la directive. Le considérant 16 ajoute que la directive ne s'applique pas aux sons et images s'ils relèvent de traitements poursuivant des fins de sécurité publique, de défense, de sûreté de l'État et de droit pénal. Le considérant 17 précise que la protection sera limitée dans l'hypothèse de traitement de sons et images à des fins de journalisme ou d'expression littéraire ou artistique. Pourtant, aucun régime spécifique n'est prévu par le texte de la directive. La limitation à la protection nécesaire à l'exercice de la liberté d'expression et à la poursuite des fins de sécurité publique sont communes à l'ensemble des données quelle que soit leur nature. L'unique article qui mentionne explicitement les sons et images est l'article 33, § 2, qui prévoit que la Commission examine en particulier l'application de la directive aux traitements de données constituées par des sons et images, relatives aux personnes physiques. Pour une analyse de l'application de la directive à la vidéosurveillance, voy. *P. de Hert, O. de Schutter* et *S. Gutwirth*, « Pour une réglementation de la vidéosurveillance », J.T., 1996, pp. 575 et 576. Concernant l'application de la Convention n° 108 aux sons et images, le Comité consultatif institué par cette Convention a considéré que les images et les voix numériques peuvent être assimilées à des données à caractère personnel (voy. T-PD(94)7, Strasbourg, Conseil de l'Europe, 1994, p. 4).

L'information est relative à une personne physique[29]. La directive reste donc fidèle à l'exclusion des personnes morales du champ d'application de la protection[30]. Elle est par contre muette sur son éventuelle application aux données relatives à des personnes physiques décédées[31].

12. La personne physique doit être identifiée ou identifiable[32]. Elle est réputée identifiable dès lors qu'une possibilité existe de l'identifier directement ou indirectement notamment par un numéro de téléphone, de plaque d'immatriculation de voiture, de sécurité sociale ou de passeport. Le texte précise par ailleurs qu'une personne peut être identifiée par référence à un ou plusieurs éléments spécifiques propres à son identité sous toute ses formes (âge, fonction professionnelle, adresse, etc.). Le but paraît ici de viser une identification issue de croisements de caractéristiques propres à certains groupes d'individus.

Se pose alors la question des données anonymes. Dans sa première version, le texte excluait les données rendues anonymes[33] par référence au critère des efforts excessifs nécessaires pour l'identification. Dans sa seconde version, le texte ne visait plus que les données agrégées sous forme statistique dès lors que les personnes concernées n'étaient plus raisonnablement identifiables[34]. Le texte actuel est dépourvu de toute précision.

29 L'article 3, §2, de la Convention n° 108 atorise quant à lui les États signataires à appliquer la Convention aux groupements de personnes physiques jouissant ou non de la personnalité juridique. Il en va de même pour le projet de recommandation du Conseil de l'Europe relative à la protection des données à caractère personnel collectées et traitées à des fins de statistiques. Le paragraphe 64 de l'annexe à la recommandation explique qu'il n'existe pas de conception objective des données personnelles relatives à des groupes humains. Si des données de groupe de personnes ayant un statut juridique (tels le couple ou la famille) sont aisément considérées comme des données à caractère personnel, il n'en va pas de même lorsque les données de groupe relèvent d'agrégation plus large (tels les habitants d'un pâté de maison) (voy. CJ-PD(97)20, p. 40).

30 Il arrive néanmoins que le traitement de données relatives à des personnes morales révèle des données personnelles. La Cour européenne des droits de l'homme a jugé de la sorte que la protection offerte par l'article 8 continue à jouer en faveur d'un individu dont les activités professionnelles et non professionnelles s'imbriquent à un point tel qu'il n'existe aucun moyen de les dissocier (pour les écoutes téléphoniques, voy. Cour eur. D.H., arrêt *Huvig*, précité, p. 41, § 8 et p. 52, § 25; pour les perquisitions, voy. Cour eur. D.H., arrêt *Niemietz* du 16 décembre 1992, série A, n° 251, p. 33, § 29; Cour eur. D.H., arrêt *Chappell* du 30 mars 1989, série A, n° 152-A, pp. 12-13, § 26). Par ailleurs, la proposition de directive RNIS va plus loin dans la mesure où elle tend à protéger les personnes morales non pas simplement en ce que le traitement de données y relatif conduirait à traiter des données personnelles, mais dans la mesure où les personnes morales elles-mêmes auraient un intérêt légitime à être protégées pour elles-mêmes (voy. proposition de directive du Parlement européenne et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de service (RNIS) et des réseaux mobiles numériques, précitée, art. 1, §2).

31 La résolution du problème semble donc être laissée à la discrétion des États (voy. The Data Protection Registrar, Questions to answers- Data protection and the EU Directive 95/46/EC, Cheshire (U.K.), Office of the Data Protection Registrar, april 1996, p. 19). Concernant la Convention n° 108, le Comité consultatif a estimé d'une part que les parties étaient libres de l'appliquer aux personnes décédées (T-PD (94)7, p. 5), d'autre part que ce texte s'applique aux foetus (T-PD (95)3. p. 5). A noter que l'article 4.5 de la recommandation R (97) 5 du Conseil de l'Europe relative à la protection des données médicales (précitée) étend la protection des données aux données de l'enfant à naître afin d'éviter, comme le précise le paragraphe 87 de l'annexe, que les données médicales d'un enfant ne soient publiques au moment de sa naissance.

32 Le rapport explicatif de la Convention n° 108 précise qu'on parlera de données personnelles lorsqu'une personne est facilement identifiable. Cela ne couvre pas l'identification des personnes par des méthodes très complexes. Une telle définition n'est plus tenable, eu égard aux possibilité informatiques de déchiffrement des mesures de cryptage ou de brouillage complexes. Comme le souligne le paragraphe 27 de l'annexe du projet de recommandation statistique du Conseil de l'Europe (CJ PD (97) 20), des données individuelles apparemment anonymes peuvent s'avérer indirectement identifiables par la combinaison de données.

33 Ce qui supposait « une modification des données à caractère personnel de sorte que les informations qui y sont contenues ne peuvent plus être associées à une personne physique déterminée ou déterminable, ou moyennant seulement un effort excessif en personnel, en frais et en temps ».

34 Pour visualiser le texte du projet initial au regard du second projet modifié, voy. la proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E., n° C 311/30, du 27 novembre 1992.

Le considérant 26 indique cependant que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mise en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier la dite personne ». Il ajoute en outre que la protection n'est pas accordée aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable. Il paraît permettre aux États membres de préciser plus avant l'exception en indiquant que les codes de conduite pourraient venir préciser les moyens à utiliser pour l'anonymisation.

13. Une difficulté surgit lorsque des moyens matériels et techniques existent aux fins d'identifier les personnes concernées alors même qu'ils ne sont pas utilisés car l'identification n'est pas nécessaire à l'activité poursuivie. Deux interprétations peuvent s'opposer.

On peut considérer que les données sont identifiables et que la protection doit être respectée. On opte alors pour la protection la plus étendue en se justifiant en termes de risque : le risque d'identification justifie par lui seul une application de la réglementation. Ce faisant, on soumet les responsables à des obligations parfois très lourdes et on crée le risque de les amener à franchir l'étape d'identification.

On peut, à l'opposé, se placer *in concreto* dans le chef de l'utilisateur des données pour apprécier en fait sa situation. Le texte français de la directive[35] y invite dès lors qu'il semble introduire une présomption. Dès lors que, techniquement, *in abstracto,* un moyen existe de rendre les personnes concernées identifiables, elles sont *réputées* telles par la définition. Le caractère identifiable apparaît alors comme relatif eu égard aux possibilités d'identification du ou des responsables. Il revient, dans cette optique, à la personne qui traite les données et qui considère ne pas devoir respecter les principes protecteurs, de rapporter la preuve du caractère anonyme de celles-ci dans son chef, en présentant toute garantie utile quant à la conservation du caractère anonyme des données[36] et susceptible de rencontrer les critères retenus par la législation nationale pour conclure à la perte du caractère identifiable des données[37].

Cette dernière position paraît être la plus réaliste. Elle responsabilise l'utilisateur des données sur qui va reposer la charge de la preuve du caractère non identifiable des données. Elle présente toutefois des difficultés en pratique car l'utilisateur doit rapporter la preuve d'un fait négatif au moyen de critères par essence difficiles à rapporter.

35 La version néerlandaise est conforme également à cette interprétation alors que la version anglaise paraît s'y opposer.

36 En mettant par exemple en exergue la mise en place d'un système permanent de codage, cryptage ou brouillage excluant la possibilité pour l'entreprise d'identifier les personnes concernées, en s'engageant dans un code de conduite ou contractuellement lors de la collecte à conserver le caractère anonyme, etc.

37 Les mêmes données pourraient être relatives à des personnes identifiables pour un responsable qui a les moyens nécessaires pour ce faire et rester anonymes pour d'autres, qui en sont dépourvus. Il paraît a priori raisonnable de dire que la réglementation ne s'applique qu'au premier et non aux seconds. Il convient en effet de ne pas confondre le problème de la définition des données à caractère personnel – données relative à une personne identifiée ou identifiable – et celui de la détermination du champ de la présomption introduite par la seconde partie de l'article 2.a. (sont réputées identifiables [...]) (Contra voy. *P. de Hert, O. de Schutter, S. Gutwirth,* Pour une réglementation de la vidéosurveillance, op. cit., p. 576, n° 25; *S. Louveaux,* in: The informed View, A business guide to changes in European data protection legislation, novembre 1996, p. 3).

II. Le traitement de données à caractère personnel

14. L'article 2, *b,* de la directive définit le traitement de données à caractère personnel comme suit: « Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés »[38].

Cette définition présente un champ d'application remarquablement large. On peut dire que toute ou ensemble d'opération(s), automatisée(s) ou non, portant sur des données à caractère personnel est visée de la collecte à l'effacement ou la destruction de celles-ci.

Elle n'implique pas d'elle-même une structuration particulière de l'information. Il en résulte que de l'information brute, présente par exemple dans un texte accessible sur un site Web, fait l'objet d'un traitement dès lors qu'elle fait l'objet d'une des opérations prévues (conservation, communication, etc.).

15. La mise en œuvre d'une telle définition suppose toutefois qu'il soit possible d'identifier, en pratique, l'existence d'un traitement spécifique. Un effort de systématisation paraît dès lors nécessaire pour apprécier la portée de cette définition.

Un traitement, quel qu'il soit, vise toujours une finalité d'utilisation précise, distincte de l'ensemble des opérations techniques effectuées. Une collecte de données, par exemple via un formulaire papier ou l'enregistrement d'informations sur un site Web, sera effectuée en vue d'opérations de marketing ultérieures. La mise en place d'un call center permettra à une entreprise d'assurances de collecter les informations transmises par l'assuré suite à un sinistre afin de le gérer. La consultation d'un site Web, reprenant par exemple, les avocats établis dans un État, tendra à une collecte d'informations à insérer dans un fichier d'adresses de contacts. Le traitement est alors constitué de l'ensemble des opérations matérielles effectuées en vue de la réalisation de la finalité recherchée.

Cette constatation a permis à de nombreux États de considérer dans leur législation interne ou dans l'interprétation des définitions que le critère de distinction d'un traitement résidait dans la finalité poursuivie par le responsable du traitement. La directive ne remet pas en cause cette conception[39].

16. Toute opération, même unique, suffit pour que l'on puisse distinguer un traitement. Ainsi, la consultation d'informations contenues dans une banque de données ou dans un texte accessible sur un site Web, sans enregistrement ultérieur, peut constituer un traitement[40].

Une telle conception, résultante d'un élargissement à outrance de la définition de traitement, aboutit à la mise en place d'une protection illusoire et affaiblit d'autant le système mis en place. En effet, elle conduit à imposer des obligations impossibles à respecter à défaut d'enregistrement et de conservation des données. Ainsi, comment la personne concernée pourrait-elle exercer ses droits d'accès et de rectification si les données ont été simplement consultées ou communiquées par un tiers sans que ce dernier ne les conserve? Quel serait l'objet d'un contrôle éventuel des autorités compétentes.

38 L'article 2, c, de la Convention n° 108 définit le traitement automatisé « comme les opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à des données, d'opérations logiques et ou arithmétiques, leur modification, leur effacement, extraction ou diffusion ». Comme le précise le paragraphe 31 du Rapport explicatif, cette définition exclut la collecte, sauf si celle-ci est effectuée à des fins d'enregistrement.

39 Le fait que dans certaines dispositions relatives au droit d'information et d'accès – art. 10, b, 11, b, 12, a – la directive parle des « finalités du traitement » est sans conséquence sur la détermination des traitements dès lors que les principes relatifs à la licéité et à la légitimité des traitements visent clairement chaque finalité distincte d'un traitement (cfr infra).

40 Le paragraphe 31, alinéa 3, du Rapport explicatif de la Convention n° 108 inclut la consultation dans la notion de traitement, pour autant, selon l'interprétation dominante, que cette consultation s'accompagne d'un enregistrement des données.

Exclure une opération unique comme la simple consultation ou la transmission[41] de données n'a pas comme conséquence de laisser la personne concernée par les données en dehors de toute protection efficace. Cette dernière peut non seulement se retourner contre le responsable du traitement qui met les données à la disposition d'autrui sur la base de la législation protectrice des données, mais également contre la personne qui utiliserait les données sans qu'un traitement n'apparaisse au sens de la réglementation et cela, en vertu des principes du droit commun (violation du droit au respect de la vie privée, du droit à l'image, du secret de la correspondance etc.). Si cette dernière introduit les informations dans un processus de traitement propre – par exemple en déchargeant tout ou partie des informations consultées dans ses propres banques de données –, la personne concernée retrouve l'intégralité de la protection accordée par la directive[42].

Il convient de remarquer que la première version du texte ne prévoyait pas que toute opération soit susceptible de constituer un traitement. Le texte actuel n'est apparu que dans la seconde version intégrant la collecte parmi les différentes opérations. On a voulu par là reconnaître à la personne concernée une protection complète dès la saisine des données par autrui même si leur traitement réel n'intervient que bien plus tard. Il a dès lors pu être jugé utile de préciser qu'une seule opération – sous-entendu la collecte – pouvait être considérée comme un traitement de manière anticipative. Ainsi, tout le processus de traitement est visé. On ne perçoit cependant pas de volonté des auteurs de la directive de retenir l'existence d'un traitement pour chaque opération unique.

III. Fichiers de données à caractère personnel

17. L'article 1, *c*, de la directive définit le fichier de données à caractère personnel comme étant « tout ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnel ou géographique »[43].

Cette définition est prévue dans le seul but de préciser la portée ou l'exclusion de certaines obligations relatives aux traitements non automatisés[44]. En effet, ces derniers ne tombent sous le champ d'application de la directive que si les données sont « contenues ou appelées à figurer dans un fichier »[45]. On exclut ainsi, comme dans la plupart des législations nationales, les dossiers non structurés du champ d'application de la directive.

41 Article 1, § 3, de la loi belge: « tout ensemble d'opérations réalisées en tout ou partie à l'aide de procédés automatisés et relatif à l'enregistrement et la conservation de données à caractère personnel, ainsi qu'à la modification, l'effacement, la consultation ou la diffusion de ces données ».

42 Le considérant 47 de la directive estime, dans le même ordre d'idées, que celui qui transmet des messages contenant des données à caractère personnel – service de télécommunication ou de courrier électronique, dont le seul objet est de transmettre des messages de ce type n'est pas un responsable du traitement. Plus fondamentalement, ce n'est pas tellement sa qualité de responsable qui paraît pouvoir être déniée – il détermine sa finalité, le transport, et les moyens techniques pour ce faire – mais bien l'inexistence d'un traitement.

43 L'article 2, b, de la Convention n° 108 définit le fichier automatisé comme « tout ensemble d'informations faisant l'objet d'un traitement automatisé ». Le paragraphe 30 du Rapport explicatif précie que cette définition « couvre non seulement des fichiers consistant en des ensembles compacts de données mais aussi des ensembles de données qui sont répartis géographiquement et réunis par l'intermédiaire d'un système automatisé à des fins de traitement ». La seule différence introduite par la directive consiste à dire que l'ensemble d'informations doit être structuré.

44 L'article 18, § 1, ne prévoit les modalités de notification à l'autorité de contrôle que pour les seuls traitements automatisés entièrement ou partiellement même si les traitements non automatisés peuvent être soumis à une telle obligation par les législations nationales; voy. également l'article 21 relatif à la publicité des traitements.

45 Article 3, § 1, de la directive.

Le critère de distinction entre le dossier et le fichier est à trouver dans le degré d'accessibilité des données à caractère personnel. La structuration de l'information à prendre en compte est centrée sur l'existence de critères relatifs aux personnes concernées[46]. Ainsi, un dossier rangé selon un critère nominatif devrait être considéré comme un fichier. La directive ne précise cependant pas « les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble »[47]. Il revient donc à chaque État de les déterminer.

Le considérant 27 précise bien que « les dossiers ou ensemble de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive ». On doute toutefois que ces précisions ~ fassent taire toute controverse à ce propos. Le nœud du problème réside encore et toujours dans la nécessaire détermination de critères d'accessibilité applicables[48]. Aucune législation ne paraît avoir, à ce jour, offert de solution excluant toute discussion. . .

IV. Le responsable du traitement et le sous-traitant

18. En vertu de l'article 2, *d*, de la directive, le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitements, de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminées par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire »[49].

La définition reprise par la directive est classique et analogue à celle présente dans les législations nationales. Il s'agit de la personne responsable des choix qui président à la définition et à la mise en œuvre des traitements. Ces choix sont relatifs aux finalités et aux moyens utilisés. Si différentes personnes ou autorités déterminent conjointement ces éléments, elles seront chacune considérées comme responsables.

Le responsable du traitement doit cependant être distingué des personnes qui procèdent aux opérations de traitement en conformité à ses instructions. Celui-ci peut ainsi faire traiter les données par les membres de son personnel ou par un sous-traitant, personne juridiquement distincte mais agissant pour son compte[50].

Si une législation ou une réglementation nationale ou communautaire précise les critères précités, elle peut en outre déterminer des modalités particulières de désignation du responsable.

46 Voy. le considérant 27 de la directive.

47 Idem.

48 Le problème se complique d'ailleurs si l'on se souvient qu'en pratique, fichiers manuels, dossiers et traitements automatisés sont étroitement liés entre eux. Ainsi, des dossiers sans véritable structure interne peuvent, via par exemple des numéros de classement et des noms, être reliés à des véritables traitements automatisés (par exemple les logiciels de gestion de la clientèle des avocats).

49 L'article 2, d, de la convention n° 108 définti le maître du fichier comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon le loi nationale pour décider quelle sera la finalité ou fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées ».

50 Article 2, e, de la directive: « La personne physique ou morale, l'autorité publique. le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ». A noter que l'article 2, e, parle de sous-traitement alors qu'il faut manifestement entendre sous-traitant. Cette notion est également une nouveauté par rapport à la Convention n° 108.

V. Le tiers et le destinataire des données

19. Le tiers est défini par l'article 2, *f,* de la directive comme toute personne autre que le responsable, le sous-traitant et les personnes placées sous leur autorité directe[51].

Il peut s'agir d'une personne physique ou morale, d'une autorité publique, d'un service ou de tout autre organisme. Dès lors que le responsable n'est pas la société elle-même ou le titulaire hiérarchique supérieur d'une entité étatique ou fédérée, un autre service ou organisme doit être considéré comme un tiers. Il en résulte par exemple que si le responsable d'un traitement est le chef du service personnel d'une société, les membres du service marketing sont considérés comme tiers.

Le tiers est parfois le destinataire des données mais pas nécessairement. Le destinataire vise toute personne qui reçoit communication des données qu'il soit ou non un tiers[52]. Les membres du personnel qui accèdent aux données dans le cadre de leur fonction sont donc des destinataires. Le texte de la directive prévoit cependant une exception en faveur des autorités « susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ». La notion de destinataire étant principalement utilisée pour déterminer le contenu des obligations d'information de la personne concernée, il s'agit vraisemblablement d'éviter au responsable du traitement de devoir rappeler à la personne concernée que, par exemple, les agents du fisc, de la sécurité sociale, etc., spécialement habilités pour ce faire, sont susceptibles d'opérer des contrôles sur les informations traitées.

VI. Le consentement de la personne concernée

20. On verra que le consentement de la personne concernée joue un rôle essentiel dans la protection mise en place. Il permet sous certaines conditions de légitimer un traitement ou de lever l'interdiction de traitement des données sensibles.

L'article 2, *h,* de la directive le définit comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant faisent l'objet d'un traitement »[53].

Toute manifestation de volonté peut constituer un consentement. Cela implique qu'il ne doit pas nécessairement être donné par écrit et qu'il peut être implicite, sauf exception prévue par la directive[54].

Le consentement doit être libre, c'est-à-dire être donné en dehors de toute pression. L'idée est de prévenir toute menace de discrimination suite au choix de la personne concernée. Cette condition, outre qu'elle peut difficilement être vérifiée, paraît bien illusoire en pratique. La pression économique consistant dans le risque de se voir refuser un produit ou un service considérés à tort ou à raison comme essentiels par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique.

Le consentement doit également être spécifique. Il ne peut avoir un objet général, mais doit porter sur des traitements précisément définis notamment en leurs finalités, poursuivies par des responsables déterminés.

51 La Convention n° 108 ne définit pas la notion de tiers.
52 Article 2, g, de la directive.
53 La Convention n° 108 ne recourt pas à la notion de consentement, mais différentes recommandations l'utilisent, telle par exemple la recommandation R (97) 5 sur la protection des données médicales.
54 Par exemple en matière de données dites sensibles (cfr infra).

Le consentement doit enfin être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. A cet égard, l'information reçue par la personne concernée au moment de la collecte semble constituer un minimum.

VII. Champ d'application matériel

21. L'article 3 de la directive détermine son champ d'application matériel.

L'article 3, § 1, énonce que la protection vise tant les traitements de données à caractère personnel automatisés, en tout ou en partie, que les traitements non automatisés de données contenues ou appelées à figurer dans un fichier[55].

L'article 3, § 2, énumère les exceptions au champ d'application. Les traitements poursuivant des finalités purement personnelles ou domestiques ne sont pas visés. De manière générale, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relatives au droit pénal sont également exclus. Plus spécifiquement, les domaines qui relèvent des titres V (politique étrangère et la sécurité commune) et VI (coopération dans les domaines de la justice et des affaires intérieures, dit troisième~) du traité sur l'Union européenne ne sont pas couverts. La protection des données est régie dans ces matières par des règles autonomes.

22. Ainsi en ce qui concerne le troisième pilier, l'article K.2 du titre VI du traité de Maastricht dispose que la politique d'asile, la politique d'immigration, l'entrée des ressortissants des pays tiers, la lutte contre la toxicomanie, la coopération judiciaire en matière civile, en matière pénale, la coopération douanière et policière seront traitées par les États membres comme des questions d'intérêt commun et l'article K.3 ajoute que les États veilleront à coordonner leur action en arrêtant des positions communes, en adoptant des actions communes et en établissant des conventions[56].

C. Lignes directrices de la protection

23. L'article 6 de la directive, intitulé « Principes relatifs à la qualité des données »[57], permettra l'analyse des principes de base de la protection : loyauté (3.A), finalité (3.B), qualité des données (3.C)[58] et légitimation des traitements (3.D).

Les régimes spécifiques aux données dites « sensibles » et aux finalités fondées sur la liberté d'expression seront ensuite examinés (3.E).

I. Le principe de loyauté

24. L'article 6, *a,* dispose que les données doivent être traitées loyalement et licitement[59].

55 L'article 3, § 1, de la Convention n° 108 limite l'application de ce texte « aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs publics et privés ».
56 L'article 14 de la Convention Europol précitée, de même que le dernier considérant du projet de Convention Eurodac, se réfèrent à la Convention n° 108. L'article 126 de la Convention d'Application de Schengen y renvoie aussi. La Convention n° 108 apparaît dès lors comme le socle commun des textes européens relatifs à la protection des données.
57 Ce titre est la transcription littérale de celui de l'article 5 de la Convention n° 108.
58 Notons dès à présent que l'article 3 permet aux États membres de prendre des mesures visant à limiter la portée de ces trois premiers principes. Ces limitations n'étant pas propres à ceux-ci, elles seront examinées gobalement infra.
59 L'article 5, a, de Convention n° 108 prévoit, quant à lui, que les données doivent être « obtenues et traitées loyalement et licitement ». Cependant, dans la mesure où l'article 2 de la directive englobe la collecte dans la notion de traitement, on peut considérer que l'article 6, a, de la directive et l'article 5, a, de la Convention n° 108 ont une portée identique.

Pour être *licite,* un traitement de données doit respecter l'ensemble des prescrits légaux découlant de la directive. La *loyauté* du traitement évoque, quant à elle, la transparence des actions. Cette transparence doit être assurée dès la collecte, notamment par le biais de l'obligation d'informer la personne concernée. Ces dernières doivent savoir quel est le but d'utilisation des données, entre quelles mains elles se trouvent, à quelles fins elles sont communiquées. Lorsque des données sont destinées à être traitées hors du territoire communautaire, le traitement ne devrait être considéré comme loyal que si l'on informe les personnes concernées des destinataires ou des catégories de destinataires des données[60].

II. Le principe de finalité

25. La doctrine a souligné l'importance du principe de finalité du traitement pour la protection de la vie privée[61]. Ce principe repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées[62].

1. La finalité doit être déterminée et explicite

26. L'article 6, *b,* précise que les données doivent être collectées pour des finalités déterminées et explicites. *A contrario,* un traitement mis en œuvre sans but précis n'est pas autorisé. Une finalité implicite doit également être exclue. Cette obligation de déterminer la finalité poursuit trois objectifs : délimiter l'atteinte aux droits et libertés individuelles, assurer la transparence du traitement et en permettre le contrôle. Diverses obligations particulières viendront concrétiser cette obligation (cfr *infra,* en particulier les obligations d'information des personnes concernées et de notification).

27. La détermination des finalités poursuit un objectif identique à l'exigence de prévisibilité de la loi imposée par la jurisprudence relative à l'article 8 de la Convention européenne des droits de l'homme. Il s'agit de circonscrire *a priori* l'étendue de l'atteinte à la vie privée en déterminant les limites dans lesquelles agit la personne qui s'ingère. Selon l'article 8 de la Convention, une atteinte à la vie privée, tel un traitement de données mis en œuvre par une autorité publique, doit être prévue par une loi qui en détermine les limites avec assez de netteté pour assurer à l'individu une protection contre l'arbitraire[63]. Un traitement de données mis en œuvre par les services de police n'est par exemple licite que si la loi qui l'autorise indique de manière suffisante en quelles circonstances et sous quelles conditions, la puissance publique est habilitée à opérer pareille atteinte secrète à la vie privée[64]. Ainsi, l'article 8 de la Convention n'autorise pas les écoutes téléphoniques à des fins de surveillance exploratoires ou générales[65].

60 L'article 10 de la directive, qui règle le droit d'information de la personne concernée, dispose à cet égard que « compte tenu des circonstances, des informations supplémentaires devront être fournies pour assurer à l'égard de la personne concernée un traitement loyal des données ».
61 Voy. *M.-H. Boulanger, C. de Terwangne et Th. Léonard,* J. T., 1993, p. 377.
62 Voy. CNIL, Dix ans d'informatique et libertés, Economica, Paris, 1988, pp. 81 et s.; voy. aussi *S. Gutwirth,* T.P.R., 1993, p. 1439.
63 Voy. Cour eur. D. H., arrêt *Malone* du 2 août 1984, précité, p. 32; et Cour eur. D. H., arrêt *Gillow* du 24 novembre 1986, série A, n° 109, p. 21.
64 Cour eur. D. H., arrêt *Malone,* précité, p. 32; Cour eur. D. H., arrêt *Leander,* précité, p. 23, § 51.
65 Cour eur. D. H., arrêt *Klass* du 6 septembre 1978, précité, p. 23, § 51.

L'obligation de détermination poursuit également un objectif de transparence : il ne peut y avoir de finalité dissimulée. La précision de la détermination devrait être appréciée in concreto, en fonction de ce que l'individu est raisonnablement censé connaître[66]. Le responsable du traitement doit avertir la personne concernée de la finalité du traitement avec d'autant plus de précision qu'il s'écarte de son activité habituelle. Ainsi, une banque ne pourrait se contenter d'affirmer qu'elle utilise les données relatives à ses clients « pour toutes les finalités légales en ce compris les finalités de marketing » alors qu'elle en fait usage à des fins de prospection d'assurance[67]. En effet, les activités d'assurance ne relèvent pas forcément des activités habituelles d'une banque et la personne concernée ne peut raisonnablement supposer que ses données seront utilisées à cette fin.

L'obligation de finalité déterminée vise enfin à permettre le contrôle de la légitimité du traitement et de la pertinence des données par une autorité de contrôle[68], que ce soit sur la base de la notification du traitement (cfr *infra*) ou à l'occasion d'une plainte.

2. La finalité doit être légitime

28. L'article 6, *b,* de la directive dispose en outre que les données doivent être collectées pour des finalités légitimes[69].

Le but même de la protection des données – le respect des libertés et des droits fondamentaux de l'individu – implique qu'une finalité de traitement ne peut violer sans justification légitime ces droits et libertés. C'est pourquoi la finalité poursuivie doit être utile et nécessaire au vu de l'objet social de l'entreprise ou de l'intérêt général. Elle ne peut non plus provoquer une ingérence excessive dans les libertés individuelles. Il convient en effet de mettre en balance l'intérêt des individus concernés à voir préserver leurs droits et libertés, et l'intérêt public ou privé à procéder au traitement des données.

L'application de la règle de proportionnalité doit permettre de vérifier que l'atteinte portée aux intérêts de la personne fichée ne soit pas excessive ou, à tout le moins, qu'elle soit compensée par la poursuite d'un intérêt supérieur du responsable du traitement[70].

29. La notion de finalité légitime est à rapprocher de l'article 8, § 2, de la Convention qui prévoit qu'une atteinte à la vie privée doit être une mesure nécessaire dans une société démocratique, à l'un des objectifs que cette disposition énumère.

La Cour européenne des droits de l'homme considère que sont seules nécessaires dans une société démocratique les atteintes pertinentes et suffisantes[71]. Une atteinte à la vie privée est pertinente si elle est utile à la réalisation d'un des buts arrêtés par l'article 8, 2, de la Convention: « Une ingérence inefficace par rapport au besoin social impérieux qu'elle était censée servir constitue une violation de la Convention »[72]. La suffisance

66 Voy. par exemple pour le degré de précision de la loi portant atteinte aux droits de l'homme: Cour eur. D. H., arrêt *Vereinigung Demokratischer Soldaten Österreich* du 19 décembre 1994, série A, n° 302, § 31; Cour eur. D. H., arrêt *Chorrer* du 25 août 1993, série A, n° 266 B, § 25.
67 Anvers, 7 juin 1994, D.C.C.R., 1994, p. 83 à 92, note *Th. Léonard;* Computerrecht, 1994, n° 4, p. 244, note *J. Dumortier et F. Robben,* D.I.T., 1994, n° 4, p. 51, note *O. Lesuisse.*
68 *M.-H. Boulanger, C. de Terwangne et Th. Léonard,* op. cit., p. 377; *S. Gutwirth,* op. cit., p. 1443.
69 Voy. l'article 5, b, de la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981.
70 *Th. Léonard, Y. Poullet* « Les libertés comme fondement de la protection des données nomitatives », in *F. Rigaux,* La vie privée une liberté parmi les autres ?, Travaux de la Faculté de droit de Namur n° 17, Bruxelles, Larcier, 1992, p. 250 et s.; *S. Gutwirth,* op. cit., p. 1439 et s.
71 Cour eur. D. H., arrêt *Dudgeon* du 30 janvier 1981, Série A n° 45, p. 28; Cour eur. D. H., arrêt *Sunday Times* du 27 octobre 1978, série A, n° 30, p. 38; Cour eur. D. H., arrêt *Olsson* du 24 mars 1988, série A, n° 130, p. 32.
72 Cour eur. D. H., arrêt *Dudgeon,* précité, § 60.

implique qu'entre différentes mesures soit choisie la moins dommageable pour la vie privée. Une mesure pertinente et suffisante doit en outre être assortie de garanties. Transposé à notre matière, constitueraient notamment des garanties le fait que la durée d'un traitement, sa finalité, sa nécessité et sa pertinence soient déterminées[73]. Enfin, une atteinte, tout en étant pertinente, suffisante et assortie de garanties, ne peut apparaître disproportionnée[74].

Ces principes ont été reconnus dans la jurisprudence de la Cour de justice des Communautés européennes qui, se référant à l'article 8 de la Convention européenne de sauvegarde, a énoncé que des restrictions peuvent être apportées à la vie privée « lorsqu'elles répondent effectivement à des objectifs d'intérêt général et qu'elles ne constituent pas, du regard du but poùvoir ; une intervention démesurée et indurable qui porterait atteinte à la substance même du droit protégé »[75].

3. La compatibilité des traitements avec les finalités

30. L'article 6, *b,* énonce que « les données ne doivent pas être traitées ultérieurement de manière incompatible avec les finalités de la collecte ». Aucun éclairage n'est apporté dans le texte même de la directive ou dans les considérants sur le sens à donner à cette disposition. L'article 5, *b,* de la Convention n° 108, qui comprend une règle identique, n'est guère plus explicite.

Au moins deux interprétations peuvent être proposées.

31. Dès lors qu'une finalité est annoncée lors de la collecte, elle doit être respectée ultérieurement. Toute opération portant sur les données trouve en effet ses limites dans la finalité déterminée, explicite et légitime annoncée. La disposition n'est donc pas nouvelle. Elle est déjà induite dans le principe de finalité lui-même. On met ici en exergue une des conséquences essentielles du principe de détermination des finalités : si l'on traite les données de manière incompatible avec le but initialement annoncé, on poursuit une finalité distincte. Si cette nouvelle finalité n'est pas déterminée au vu et au su des personnes concernées ou des tiers, il y a un détournement de finalité. La règle n'empêche donc pas l'évolution ultérieure des traitements par rapport aux finalités annoncées lors de la collecte. On peut changer de finalité, mais alors, on doit y voir un nouveau traitement soumis intégralement à la réglementation.

Cette interprétation paraît conforme à une recherche de la *ratio* du texte commenté. Le sens ne peut être à trouver, vu l'objet de cette matière, que dans la protection recherchée pour la personne concernée par les données. L'idée semble être qu'il faut éviter que des données obtenues en annonçant une finalité particulière soient utilisées pour un tout autre but. On retrouve ici la crainte des détournements de finalités. Un détournement suppose que le changement de finalité soit opéré à l'insu de la personne concernée, sans que cette dernière puisse réagir. Le responsable du traitement doit donc toujours être attentif à faire connaître à la personne concernée les finalités réellement poursuivies sans en masquer l'une ou l'autre.

73 Cour eur. D. H., arrêt *Klass,* précité, p. 24.

74 Voy. *J. O. Viout,* « La Cour européenne des droits de l'homme et le principe de proportionnalité », in Le principe de proportionnalité en droit belge et français, Liège, éd. du Jeune Barreau de Liège, 1995, p. 187 et s. L'auteur n'hésite pas à qualifier le contrôle exercé par la Cour de contrôle de pure opportunité. Voy. aussi *M. A. Eissen* « Le principe de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », in *L. E. Pettiti, E. Decaux, P. A. Imbert,* La Convention européenne des droits de l'homme, op. cit, p. 65 et s.

75 C.J.C.E., 5 octobre 1994, précité (note 21).

32. Une autre interprétation pourrait également être soutenue. Plutôt que de n'autoriser que les utilisations des données qui s'inscrivent dans les finalités annoncées au moment de la collecte, sous peine de se trouver en présence d'un nouveau traitement (avec tout ce que cela implique comme formalités d'information, de notification, etc. cfr. *infra*), l'article 6, *b,* peut se lire comme admettant tous les changements de finalité compatibles avec les buts annoncés initialement, sans y voir la création de nouveaux traitements. Il faut toutefois rappeler que la finalité initiale doit être explicite, ce qui réduit considérablement l'étendue des finalités compatibles.

Pour appréhender la portée de la règle et éclairer davantage la notion de compatibilité, on pourrait notamment se référer utilement à l'attente raisonnable des personnes concernées au vu de la finalité première. Une finalité de marketing de produits bancaires paraît ainsi incompatible avec une finalité d'évaluation du risque du crédit à accorder. Lorsque la personne fournit ses données pour l'évaluation du risque, elle ne s'attend pas raisonnablement à ce que les informations transmises puissent être automatiquement utilisées pour des finalités de prospection. Toute difficulté n'est toutefois pas écartée.

Ainsi, quel est le sort d'une nouvelle finalité réputée « compatible » ? Autrement dit, la compatibilité permet-elle de faire l'économie d'un contrôle de légitimité appliqué au but nouvellement poursuivi ? Si l'on répond par l'affirmative, on confisque à la personne concernée toute protection vis-à-vis de la nouvelle finalité. Ainsi, dans le cas où une communication des données à un tiers – opérée par exemple lors d'un échange de fichiers clientèles ou de membres d'une association – serait jugée compatible avec une finalité de gestion de la clientèle et de marketing des produits ou services offerts, la personne concernée ne pourrait plus s'opposer à la communication en contestant la légitimité de celle-ci. La compatibilité serait donc en quelque sorte un blanc-seing permettant d'éviter un contrôle de légitimité. Est-ce réellement le but des rédacteurs de cette disposition ? Il est assurément permis d'en douter.

Par ailleurs, qu'advient-il des utilisations de données incompatibles avec les finalités annoncées lors de la collecte de celles-ci ? Doit-on lire l'article 6, *b,* comme les interdisant purement et simplement ? Cela figerait une fois pour toutes les finalités des traitements au moment de la collecte. Des données collectées par une société d'assistance à des personnes voyageant à l'étranger dans le but unique de gérer ce service ne pourraient pas être utilisées ultérieurement – suite à une diversification des activités – dans un but de marketing d'un nouveau produit d'assistance des personnes âgées. Une telle interprétation ne paraît pas raisonnable. Les traitements ne constituent généralement pas des fins en eux-mêmes, mais bien les supports d'activités économiques ou d'intérêt général. Ces activités doivent se transformer en fonction de l'évolution des besoins. S'y opposer sur la base de la protection des données est disproportionné par rapport à l'élément de protection recherché. Le fondement de la protection n'est pas à trouver dans le refus de changement des finalités, mais dans la nécessité de soumettre tous les traitements aux principes fondamentaux de la protection. L'important est donc d'éviter que la personne concernée ignore ces modifications et ne puisse, le cas échéant, s'y opposer. Il faut sans doute voir dans les utilisations incompatibles la mise en œuvre de traitements nouveaux générant l'ensemble des obligations liées à tout traitement en tant que tel.

33. En conséquence, la transposition en droit interne d'une telle disposition suscitera vraisemblablement des débats sans doute difficiles. On ne peut à ce stade que regretter que les auteurs de ce texte n'aient pas franchement posé le problème des transformations de finalités, très fréquentes en pratique. C'est d'autant plus étonnant que cer-

taines législations nationales, dont la loi belge, possédaient une règle particulière d'information dans cette hypothèse[76].

34. L'article 6, *b,* précise enfin que n'est pas réputé incompatible un traitement ultérieur à des fins historiques, statistiques ou scientifiques, pour autant que les États membres prévoient des garanties appropriées. Selon le considérant 29, les garanties appropriées doivent notamment empêcher les mesures ou décisions prises à l'encontre d'une personne sur base de ces traitements. Pour élaborer celles-ci, les États membres se réfèreront utilement à la future recommandation du Conseil de l'Europe sur la protection des données à des fins statistiques et au règlement communautaire relatif à la statistique communautaire[77].

III. Les principes de qualité des données

35. L'article 6, *c,* dispose que les données doivent être adéquates et pertinentes par rapport aux finalités[78]. On vise ici une liaison nécessaire et suffisante de l'information par rapport à la finalité. Il est vrai que, bien souvent, cette obligation rejoint le souci de rationalisation du responsable du traitement qui désire normalement ne conserver que des informations utiles à ses activités.

En pratique, un audit, révèle que bon nombre de données sont seulement conservées ou enregistrées pas habitude alors qu'elles ne présentent par réellement d'utilité pour un traitement. Il convient alors de les supprimer. La règle va cependant plus loin. Ainsi, elle implique également qu'une donnée ne soit pas conservée dans le système si le but recherché peut être atteint autrement, par un moyen moins dommageable pour les libertés individuelles. Cela pourrait être le cas si l'identification d'une personne peut être garantie autrement que par la conservation d'un numéro d'identification nationale.

36. Par ailleurs l'article 6, *c,* précise que les données ne doivent pas être excessives au regard de la finalité poursuivie. Seraient-elles adéquates et pertinentes, les données ne peuvent néanmoins pas faire l'objet d'un traitement si elles provoquent une atteinte disproportionnée aux intérêts de la personne concernée. Il peut s'avérer utile pour un organisme de crédit de traiter des données médicales relatives à des candidats à l'ouverture de crédit afin de sélectionner le risque; toutefois, un tel dévoilement d'informations touchant à l'intimité des individus peut s'avérer excessif. Seul le traitement de certaines données médicales pourra, le cas échéant, être justifié au vu de la nature et de l'ampleur des prêts envisagés.

37. L'article 6, *d,* dispose que les données doivent être exactes et, si nécessaire, mises à jour[79]. Il précise que « toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes au regard des finalités par lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées ». Il s'agit donc clairement d'une obligation de moyens. Le critère à prendre en compte sera donc celui du responsable normalement prudent et diligent.

76 Article 9 de la loi du 8 décembre 1992; sur ce dernier, voy. *M.-H. Boulanger, C. de Terwangne et Th. Léonard,* op. cit., p. 382.
77 Règlement n° 322/97 du Conseil du 17 février 1997 relatif à la statistique communautaire, précité.
78 L'article 5, c, de la Convention n° 108 est libellé de manière identique.
79 Cet article reprend le libellé de l'article 5, d, de la Convention n° 108.

38. Enfin, l'article 6, *e,* prévoit que « les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées ultérieurement »[80].

On retrouve ici ce qu'on appelle communément le droit à l'oubli de la personne concernée par les données. L'idée sous-jacente est qu'une donnée conservée pour une durée excédant un délai raisonnable peut être considérée comme non pertinente ou excessive eu égard à la finalité poursuivie.

IV. Les principes de légitimation des traitements

39. L'article 6, *b,* impose que les finalités soient légitimes et que les données ne soient pas excessives par rapport à ces finalités. Il faut admettre que ces conditions abstraites – débouchant sur l'imposition d'un critère de proportionnalité – sont particulièrement difficiles à appréhender et peu éclairantes pour la plupart des responsables du traitement. C'est sur ce point que la directive vient innover en précisant explicitement les règles de base de la légitimation des traitements[81].

L'article 7 indique en effet des situations – les plus fréquentes en pratique – où la règle de proportionnalité est *a priori* respectée. Les traitements seront normalement admis s'ils trouvent leur fondement soit dans le droit privé – par un contrat (7, *b*) ou le consentement de la personne concernée (7, *a*) – soit dans le droit public –, par une obligation imposée par la loi (7, *c*) ou par la poursuite par l'État d'une mission d'intérêt public (7, *e*), soit enfin dans l'inrérêt vital de la personne concernée (7, *d*). Un dernier fondement est l'intérêt prépondérant du responsable du traitement ou d'un tiers à qui sont communiquées les données (7, *f*). Dans le même temps, l'article 7 prévoit des conditions spécifiques assurant *a priori* un équilibre entre les intérêts de la personne concernée et du responsable du traitement.

En dehors de ces conditions, aucun traitement de données ne peut avoir lieu. La formule introductive de l'article 7 ne laisse pas aux États membres la latitude d'imaginer d'autres hypothèses ni d'exclure l'une d'entre elles[82]. Par contre, en vertu de l'article 5, ils sont libres d'être plus exigeants dans la formulation de l'une des hypothèses.

40. Le traitement peut d'abord être poursuivi « si la personne concernée a indubitablement donné son consentement ». Le consentement dont il s'agit doit bien évidemment répondre aux conditions contenues dans la définition donnée en préliminaire par la directive[83].

L'insertion de l'adverbe « indubitablement» permet d'admettre les consentements qui, sans nécessairement être exprès, n'en sont pas moins certains. Le traitement se justifie également *a priori* s'il est « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».

80 L'article 5, e, de la Convention n° 108 dispose également que « les données sont conservées sans une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées ». Le rapport explicatif de la Convention n° 108 souligne que cela ne signifie pas qu'elles doivent être séparées après quelque temps irrévocablement du nom de la personne à laquelle elle se réfèrent, mais seulement qu'il ne doit pas être possible de relier facilement les données et les identifiants.
81 Le projet de recommandation du Conseil de l'Europe, relative à la protection des données a carectère personnel à des fins d'assurance reprend cette démarche en distinguant les conditions de licéite des conditions de légalité (voy. CJ-PD, [97] 28, p. 5).
82 L'article 7 énonce que « les États membres prévoient que le traitement des données à caractère personnel ne peut être effectué que si (. . .) », suivent alors les différentes situations.
83 Voy. supra, n° 20.

Dans ce cas, le responsable devra s'assurer que le traitement est réellement nécessaire à la conclusion ou l'exécution du contrat, c'est-à-dire que la finalité du traitement vise l'essence même des mesures précontractuelles ou de l'objet des prestations. Sur cette base, une banque ne pourra pas forcément établir des profils de consommation de ses clients à partir de l'utilisation de leur carte de crédit, dans le cadre du contrat de fourniture du service.

La disposition permet aussi le traitement de données nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis. On peut citer à titre d'exemple des obligations qui s'imposent aux employeurs, telles la tenue d'une comptabilité particulière ou d'un registre du personnel accessible aux inspecteurs chargés du contrôle de la législation sociale, la communication de certaines données de leur personnel aux organismes de sécurité sociale, etc.

Le traitement des données est également permis s'il est « nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ». Le considérant 31 de la directive précise qu'on vise la protection d'« d'un intérêt essentiel à la personne concernée » . Cette disposition pourrait fonder le traitement de données dans les cas où la personne concernée se trouve dans une situation d'urgence médicale[84].

Le traitement peut être aussi fondé s'« il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou les tiers auquel les données sont communiquées ». On vise ici les traitement poursuivis dans le secteur public au sens large. Si l'on effectue le rapprochement avec la règle de légitimité, on retrouve les principes administratifs de légalité, spécialité et proportionnalité[85]. Il arrive que dans la poursuite de ses missions prévues par la loi, l'administration soit amenée à porter atteinte aux libertés individuelles. Pareille atteinte doit être proportionnelle, c'est-à-dire suppose qu'une relation raisonnable existe entre le but poursuivi et les moyens mis en œuvre pour l'atteindre, ce qui est excessif devant être taxé non seulement d'inopportun, mais d'illégal[86]. Le principe de proportionnalité oblige l'autorité administrative d'une part, à examiner les intérêts en présence avant de prendre une décision – la motivation de la décision devant faire apparaître la mise en balance – et d'autre part, à prendre un acte conforme à cette balance[87].

Enfin, l'article 7 admet la mise sur pied d'un traitement s'« il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les biens auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ». Cette disposition diffère quelque peu des hypothèses précédentes. Alors que ces dernières précisaient des situations où l'équilibre des intérêts en présence est *a priori* respecté, la présente disposition rappelle de manière plus explicite le contenu même de la règle de proportionnalité inhérente au principe de légitimité. Même si le traitement est nécessaire au responsable, il ne pourra être poursuivi dès lors que l'opposition des intérêts en présence se résout en faveur de la personne concernée. Ce faisant, on perçoit encore mieux

84 Contrairement au traitement de données sensibles, le responsable ne doit pas prouver dans ce cas, que la personne concernée se trouvait dans l'incapacité physique ou juridique de donner son consentement (article 8, § 2, c).

85 Voy. *Th. Léonard, Y. Poullet* « Les libertés comme fondement de la protection des données nominatives », op. cit., p. 242, n° 15 et 260, n° 43; il faut par ailleurs ne pas perdre de vue les exigences de l'article 8, § 2, de la Convention européenne des droits de l'homme.

86 *O. Daurmont et D. Batsele* « Cinq », Adm. publ., 1990, p. 274.

87 *P. Lewalle,* Le principe de proportionnalité dans le droit administratif, Adm. Publ., 1995, p. 53; *R. Andersen,* Le juge du l'excès de pouvoir et la mise en balance des intérêts en présence, in *Ph. Gérard, F. Ost, M. van de Kherkove,* Droit et intérêt, Bruxelles, FUSL, 1990, p. 144.

la nature explicative de l'article 7 qui a pour objectif principal d'éclairer le contenu des exigences du principe de légitimité des traitements.

41. L'articulation entre les article 6 et 7 précités doit être bien comprise.

Le fait de remplir une des conditions de l'article 7 n'implique pas que l'exigence de légitimité de l'article 6, ni aucune autre de ses règles, soit *ipso facto* rencontrée. Les deux dispositions doivent au contraire s'appliquer cumulativement.

C'est ce que rappellent les considérants de la directive : tout traitement doit poursuivre une finalité légitime et respecter les autres exigences de l'article 6[88], mais pour être licite, il doit, en outre, être fondé sur une des situations reprises à l'article 7[89]. Si les règles de l'article 7 doivent être nécessairement respectées, les obligations qui en découlent ne permettent pas de faire l'économie de l'application des autres conditions de licéité contenues dans l'article 6. Ainsi, le consentement de la personne concernée ne permet pas nécessairement – même si ce sera souvent le cas – de légitimer la finalité du traitement[90].

Si l'on veut pousser plus avant la comparaison entre les deux dispositions, on pourrait dire que l'article 7 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté, sans préjudice d'un contrôle concret, issu de l'article 6, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu.

V. Catégories particulières de traitement

42. La directive prévoit des règles de protection particulières en ce qui concerne les traitements de certaines données dites « sensibles » (E.*a*) et les traitements se fondant sur la liberté d'expression (E.*b*).

1. Les traitements de données « sensibles »

43. Deux catégories de données font l'objet d'une réglementation particulière.

Tout comme l'article 6 de la Convention n° 108[91], l'article 8 de la directive part du principe que les traitements portant sur certaines données sont *a priori* interdits. Ces données sont limitativement énumérées. Un régime commun est établi pour celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. On retrouve ici les données dites « sensibles » au sens le plus classique.

D'autres données ne peuvent être traitées que sous certaines conditions spécifiques. Certaines de ces conditions, très générales, sont déterminées par la directive, les autres sont laissées à la discrétion des États membres. Il s'agit des données relatives aux infractions, aux condamnations pénales ou mesures de sûreté, aux sanctions administratives,

88 Considérant 28 de la directive.

89 Considérant 30 de la directive.

90 Le fait que l'article 6, b, de la directive parle de finalités légitimes et que l'article 7 soit intitulé « Principes relatifs à la légitimation des traitements de données » pourrait laisser croire le contraire (voy. également la version anglaise). Le texte néerlandais de la directive lève l'ambiguïté. En son article 6, il dispose que « De Lid Staten bepalen dat de persoonsgegevens voor een welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinde moeten worden verkregen... (...) » alors que l'article 7 est intitulé « Beginselen betreffende de toelaatbaarheid van gegevensverwerking ». Autrement dit, l'article 7 n'indique que des principe d'admissibilité du traitemement sans préjudice des autres dispositions de la directive.

91 Les catégories de données diffèrent cependant quelque peu. L'article 6 de la convention n° 106 n'inclut pas l'appartenaire syndicale.

aux jugements civils ainsi que les numéros d'identification nationale ou autre identifiant de portée générale. On vise donc ici principalement les données dites « judiciaires ».

44. Le principe d'interdiction de traitement des données de la première catégorie souffre un grand nombre d'exceptions prévues précisément ou non par le texte même de la directive[92].

L'article 8, § 2, *a*, autorise le traitement de données sensibles « lorsque la personne concernée a donné son consentement explicite à un tel traitement »[93].

Les États membres disposent cependant d'une grande marge de manœuvre puisqu'ils peuvent prévoir que, dans les cas qu'ils déterminent, le consentement ne lève pas l'interdiction. On peut s'attendre à ce que les États membres optent pour une telle possibilité dans les nombreuses hypothèses où le consentement libre de la personne concernée est illusoire vu la nature particulière des relations entre celle-ci et le responsable du traitement : données sensibles relatives à un membre du personnel traitées par son employeur, données sensibles exigées par les assureurs ou tout autre prestataire d'un service devenu nécessaire économiquement ou socialement dans nos sociétés modernes, données sensibles traitées par une autorité publique, etc.

Le consentement doit répondre aux exigences de la définition arrêtée de manière générale par la directive[94]. Il doit en outre être explicite, mais ne doit pas forcément être donné par écrit.

L'article 8, § 2, *b*, lève l'interdiction de traiter des données sensibles si le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail[95].

En son point *c*, l'article 8, § 2, permet le traitement de données sensibles lorsque le traitement est nécessaire à l'intérêt vital de la personne concernée ou, dans les cas où cette dernière se trouve dans l'incapacité physique ou juridique de donner son consentement, d'une autre personne[96].

En vertu du point d de la même disposition, une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale peuvent également traiter des données sensibles si le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées, pour autant que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées. Cependant, seules les données sensibles relatives aux membres de ces organismes et aux personnes entretenant des contacts réguliers liés à la finalité du traitement sont visées. Cette exception paraît particulièrement vague. On peut se demander quelles pourraient être les garanties dont question dès lors qu'elle seraient différentes de celles prévues explicitement. On perçoit mal également comment déterminer les personnes liées à la finalité d'un traitement : n'est-ce pas toujours le cas des personnes concernées par les données ?

92 La convention n° 108 quant à elle, interdit le traitement de données sensibles à moins que le droit interne ne prévoie des garanties appropriées, cette dernière expression recouvrant les mesures protégeant les données sensibles qui vont au-delà de la protection minimale accordée aux données non sensibles (voy. CT-PD, [93] 5, p. 7).

93 L'article 4.3. C. iii de la recommandation R (97) 5 relative à la protection des données médicales (précitée) dispose de manière similaire que « les données médicales peuvent être collectées et traitées si la personne concernée ou son représentant légal ou une autorité de contrôle ou toute autre personne ou instance désignée par la loi y a consenti, pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas ».

94 Voy. supra, n° 20.

95 Il est à noter que si les articles 4.3.b.iii et 7.3.b. iii de la recommandation R (97) 5 du Conseil de l'Europe relative à la protection des données médicales autorise leur traitement dans le cadre d'obligations contractuelles, l'alinéa 6 du point 74 de l'annexe à la recommandation précise que « lors du traitement de données, dans le cadre des obligations contractuelles, les États membres de la Communauté ne pourront après transposition de la directive communautaire dans leur législation nationale, faire usage de cette faculté que dans le contexte du droit du travail. Pour les autres membres du Conseil de l'Europe, ces dispositions peuvent entrer en ligne de compte dans d'autres domaines, tel que le sport, la formation ou les assurances ».

Sont aussi visés par la levée de l'interdiction les traitements portant sur des données manifestement rendues publiques par la personne concernée et ceux nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

L'article 8, § 3, de la directive autorise finalement le traitement de données sensibles à des fins médicales (médecine préventive, diagnostic médical, administration de soins de santé ou de traitements) et à des fins de gestion des services de santé[97]. Si cette disposition permet le traitement de données sensibles dans le cadre de la relation thérapeutique, elle ne semble pas pouvoir couvrir les traitements de données dans les expérimentations médicales (essais cliniques de médicaments, essais d'appareils, etc.). En outre, il faut que le traitement soit effectué par un praticien de la santé soumis au secret professionnel, ou par une autre personne soumise à une obligation de secret équivalente.

L'article 8, § 4, permet également aux États membres d'autoriser, pour un motif d'intérêt public important, d'autres cas de traitements portant sur des données sensibles à condition que ces traitements soient accompagnés de garanties appropriées[98]. Le considérant 34 indique comme exemple de domaines où l'intérêt public pourrait justifier la levée de l'interdiction la santé publique et la protection sociale[99], la recherche scientifique et les statistiques publiques. On risque donc de voir apparaître dans ces matières des divergences importantes entre États membres.

45. En ce qui concerne les données judiciaires, l'article 8, § 5, distingue selon la nature de celles-ci. Les données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peuvent être normalement traitées que sous le contrôle de l'autorité publique en prévoyant des garanties appropriées et spécifiques. Toutefois, les États membres peuvent prévoir des exceptions[100] et permettre, par exemple, que des sociétés privées, comme des banques ou sociétés d'assurances, traitent ces données s'ils prévoient des garanties particulières.

Les données judiciaires relatives aux sanctions administratives et civiles peuvent également être traitées sous le contrôle de l'autorité publique si l'État membre en décide. Le texte ne précise pas si des garanties appropriées et spécifiques doivent être arrêtées. Une interprétation littérale du texte implique que les États membres ne puissent permettre leur traitement en dehors du contrôle de l'autorité publique. On comprend mal ce qui justifie ici un régime plus strict que pour les données à caractère pénal.

La directive s'en remet enfin aux États membres pour prévoir les conditions dans lesquelles un numéro d'identification national ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. On peut donc en conclure que ces données ne peuvent pas être utilisées en dehors d'une réglementation précise.

96 Voy. supra, n° 40.

97 L'article 4.4. de la recommandation relative à la protection des données médicales précitée prévoit également que les données médicales puissent être traitées à des fins de gestion de service de santé. Il précise néanmoins que « la gestion est fournie par le professionel de la santé qui a collecté les données ».

98 Les dérogations au principe d'interdiction doivent toutefois être notifiées à la Commission.

99 Le considérant 34 précise qu'il vise principalement les cas où il s'agit d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie.

100 Cette disposition précise qu'un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

46. Les difficultés qui surgiront lorsque les États membres devront transposer en droit interne les dispositions de l'article 8 sont en grande partie identiques à celles rencontrées antérieurement au sein de chaque État membre.

Le principe d'interdiction pose des problèmes insolubles de légistique. On a beau faire preuve de prévoyance en énonçant une kyrielle d'exceptions, la liste devra être indéfiniment complétée par des hypothèses où le traitement des données sensibles paraît légitime même si elles ne s'insèrent pas dans celles déjà arrêtées. La directive, malgré son effort de systématisation, n'évitera pas le même écueil.

La difficulté sera cependant encore plus aiguë dès lors que les possibilités laissées par l'article 8, § 4, aux États membres d'étendre les exceptions sont par essence limitées. Accroître les exceptions en dehors de la marge de manœuvre laissée aux États aurait pour conséquence d'amoindrir la protection désirée élevée ou de créer des brèches trop importantes à l'équivalence recherché des niveaux de protection.

Paradoxalement, certaines exceptions frappent par leur imprécision. On pourra alors être amené à profiter de celle-ci pour les interpréter de la manière la plus extensive en vue d'y insérer des hypothèses non expressément visées. Ce faisant, on permet à des traitements réellement problématiques de passer entre les mailles de la protection.

Un autre effet pervers risque enfin de se présenter. Afin d'étendre les exceptions, les États membres risquent de se contenter de lever l'interdiction par la voie du consentement dans des hypothèses où ce dernier est un leurre.

2. Les traitements de données à caractère personnel et la liberté d'expression

47. L'article 9 de la directive impose aux États membres de prévoir des exemptions et des dérogations aux principes fondamentaux de la protection mise en place « dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ». Dans le même temps, la disposition précise cependant que seuls sont visés « les traitements de données à caractère personnel effectuées aux seules fins de journalisme ou d'expansion artistique ou litéraire ».

Ces exemptions et dérogations ont, *a priori,* un champ d'application extrêmement large puisqu'en réalité, c'est la presque intégralité des règles de la directive qui peuvent ainsi être réduites à néant : les principes de licéité des traitements[101], les dispositions relatives au transfert de données à caractère personnel vers des pays tiers[102] et aux autorités de contrôle et groupe de protection[103]. En bref, parmi les règles directes de protection, seules les dispositions générales contenant les définitions et précisant le champ d'application de la directive ainsi que les règles relatives aux recours et sanctions ne peuvent être énervées au nom de la liberté d'expression.

48. L'élan des États membres sera toutefois bridé par le critère de nécessité et la définition restrictive des finalités de traitements pour lesquels une exception à la protection est possible. Dans le cadre d'un commentaire général de la directive, trois seules réflexions seront faites sur ces limitations.

101 Chapitre 2 de la directive comprenant les dispositions relatives à la qualité des données (article 6), à la légitimation des traitements (article 7), aux données dites « sensibles » (article 8), à l'information de la personne concernée (articles 10 et 11), au droit d'accès (article 12), aux exceptions et limitations de l'article 13, au droit d'opposition de la personne concernée (articles 14 et 15), à la confidentialité et la sécurité des traitements (articles 16 et 17), à la notification, aux contrôles préalables et à la publicité des traitements (articles 16 à 21).

102 Articles 25 et 26 de la directive.

103 Articles 28 à 30 de la directive.

Les États membres ne peuvent *a priori,* au nom de la liberté d'expression, exclure du champ d'application de leur législation nationale les traitements visés par la directive, ni les soumettre entièrement à celle-ci. L'article 9 de la directive contient explicitement une obligation faite aux États de garantir un équilibre entre les deux libertés opposées.

La seule mesure de cet équilibre est à trouver dans la nécessité d'une conciliation entre les deux libertés concurrentes. Si des exceptions s'imposent d'elles-mêmes pour permettre l'exercice de la liberté d'expression – le secret des sources ne peut être réduit à néant par le droit à l'information reconnu à la personne concernée, le contrôle des journalistes ou entreprises de presse par les organes spécialement institués ne peut devenir l'instrument indirect d'une censure, etc. –, les principes de protection pourront être plus largement respectés une fois que la liberté d'expression a été pleinement exercée, c'est-à-dire une fois que les informations contenues dans les traitements ont été publiées ou mises à la disposition du public. On pense par exemple aux banques de données reprenant tout ou partie des informations publiées dans la presse écrite ou contenues dans des livres éditées.

La marge de manœuvre des États membres reste très importante. Ces derniers pourront tant jouer sur l'interprétation des finalités des traitements énoncées par le texte – qu'est-ce qu'une finalité journalistique ? – que sur une interprétation propre du critère de nécessité lui-même. Un critère d'unification pourra cependant être utilement trouvé dans la jurisprudence de la Cour européenne des droits de l'homme afin de jauger le poids de chacune des libertés qui s'entrechoquent au travers de l'application des principes protecteurs de la directive.

D. Les droits de la personne concernée et obligations du responsable du traitement

49. Après avoir posé les principes de base de la protection de l'individu, la directive organise le contrôle de leur application. D'une part, elle garantit la transparence du traitement des données à caractère personnel par le biais de l'obligation d'information de la personne concernée, mise à charge du responsable du traitement (A). D'autre part, elle consacre différents droits pour la personne concernée lui permettant de conserver une relative maîtrise des données à caractère personnel la concernant. Les droits d'accès et de rectification retiendront d'abord l'attention (B). La directive introduit des exceptions générales à ces droits ainsi qu'à l'obligation d'information (C). Le droit d'opposition sera ensuite étudié (D). Enfin, la directive prévoit que la personne concernée ne peut être sujette à des décisions individuelles automatisées (E). Par ailleurs, une obligation de notification des traitements automatisés à l'autorité de contrôle nationale est instaurée (F) et des obligations de sécurité des traitements sont mises à charges des responsables du traitement (G).

50. En principe, il appartient au responsable du traitement, voire à son représentant d'assurer le respect de ces droits et obligations. L'idée est d'élire un responsable unique du traitement, interlocuteur privilégié de la personne concernée.

I. L'information de la personne concernée

51. Le responsable du traitement a l'obligation d'informer la personne concernée sur les caractéristiques principales des traitements qu'il poursuit. Cette obligation permettra à la personne concernée d'exercer effectivement ses droits et de donner, le cas échéant, son consentement éclairé. Le respect de cette obligation d'information incombe au responsable du traitement ou à son représentant. Ces derniers sont toutefois dispensés de renseigner la personne concernée « lorsque celle-ci est déjà informée ».

Les informations de base concernant l'identité du responsable du traitement[104] et les finalités des traitements devront toujours être transmises sauf si l'État membre fait application des exceptions générales prévues à l'article 13 de la directive. D'autres informations seront le cas échéant transmises à la personne concernée, selon les règles indiquées ci-après.

52. Les modalités et l'objet de l'obligation d'information diffèrent selon que cette dernière est destinée ou non à une personne ayant directement transmis au responsable du traitement les données à caractère personnel la concernant.

Dans la première hypothèse, l'information se fera au moment même de la collecte auprès de la personne concernée[105]. En plus des informations de base, le responsable du traitement devra, le cas échéant, indiquer les destinataires ou catégories de destinataires des données, le caractère obligatoire ou facultatif des réponses ainsi que les conséquences d'un défaut de réponse, et mentionner l'existence des droits d'accès et de rectification des données.

Dans la seconde hypothèse, c'est-à-dire celle où les données n'ont pas été collectées auprès de la personne concernée, l'information devra être fournie dès l'enregistrement des données ou, si une communication des données à un tiers est envisagée, au plus tard lors de la première communication des données[106]. Les informations supplémentaires portent sur les destinataires ou catégories de destinataires des données, l'existence des droits d'accès et de rectification et les catégories de données concernées. Une exception particulière est ici prévue pour les traitements à finalité statistique et de recherche historique ou scientifique à condition que l'information de la personne concernée se révèle « impossible ou implique des devoirs disproportionnés, ou si la législation prévoit expressément l'enregistrement ou la communication de données ». Dans ces cas, les États membres prévoient des garanties appropriées[107].

53. En toute hypothèse, la directive précise que les informations supplémentaires ne seront transmises à la personne concernée que dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Le texte de la directive ne spécifie pas quelles sont ces circonstances particulières. La loyauté doit être comprise au sens de l'article 6 de la directive, et renvoie dès lors à l'exigence de transparence. Les informations supplémentaires sont nécessaires dans la mesure où la personne concernée doit voir son attention attirée sur les risques spécifiques générés par le traitement en cause à l'égard de ses libertés individuelles (traitement de données sensibles, traitement de données dans le cadre d'un réseau ouvert, transmission de données vers des pays tiers n'assurant pas un niveau de protection adéquat, etc.)[108]. Ainsi par exemple, si les données sont destinées à être communiquées à des tiers autres que ceux auxquels la personne peut raisonnablement s'attendre, ceux-ci devront être spécifiés. C'est au responsable du traitement qu'il appartient dans un premier temps d'évaluer si la fourniture de telles informations est nécessaire, sous le contrôle en particulier des autorités nationales de protection des données.

104 Le cas échéant, de son représentant (cf. article 10 de la directive).
105 Article 10 de la directive.
106 Article 11 de la directive.
107 Article 11, § 2, de la directive. L'article 9, § 3, de la Convention n° 108 autorise également des restrictions au droit d'information pour les fichiers utilisés pour des recherches statistiques ou scientifiques « pour autant qu'il n'existe manifestement pas de risque d'atteinte à la vie privée ».
108 Voy. *C. de Terwangne, S. Louveaux*, « Data protection and online networks », Computer Law & Security Report, 1997, vol. 13, n° 4.

Enfin, la directive reste muette quant à la procédure d'information elle-même. Il reviendra donc aux États membres de déterminer la forme qu'elle doit respecter (orale, écrite, collective, etc.).

II. L'accès et la rectification des données

54. Afin de contrôler la qualité des données la concernant (qu'elles soient complètes, exactes, mises à jour) et de vérifier le respect des règles découlant du principe de finalité, la directive confère à la personne concernée un droit d'accès aux données à caractère personnel se rapportant à elle[109]. Ce droit doit être exercé sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs.

La personne concernée doit ainsi pouvoir obtenir la confirmation que ses données personnelles sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées.

La personne concernée se voit également reconnaître le droit d'obtenir la communication, sous une forme intelligible, des données faisant l'objet du ou des traitements, ainsi que toute information « disponible » sur l'origine des données. Cette dernière obligation apparaîtra comme primordiale lorsque les données n'ont pas été directement collectées auprès de la personne concernée[110].

55. Du droit d'accès dérive le droit d'obtenir, selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, notamment en raison de leur caractère incomplet ou inexact[111].

Ce droit de rectification est donc particulièrement étendu. Toutes les règles de la directive sont *a priori* visées sans exception : respect du principe de finalité, des règles de sécurité, de l'obligation de notification, etc. Le problème sera dès lors de veiller à une proportionnalité entre la gravité du manquement et la « sanction » demandée par la personne concernée. Il pourrait, par exemple, paraître insensé d'imposer l'effacement des données suite au non-respect de l'obligation de notification auprès de l'autorité de contrôle. Un verrouillage jusqu'à la mise en ordre du responsable du traitement paraîtrait par contre plus raisonnable.

La directive laisse la charge de la preuve des manquements à la personne concernée par les données, ce qui en pratique enlève à ce droit une grande partie de son contenu.

Le responsable du traitement doit, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné, notifier aux tiers auxquels les données ont été communiquées les rectifications, effacements ou verrouillages effectués[112]. Le texte ne précise toutefois pas si le tiers est lui-même obligé de répercuter ceux-ci dans ses propres traitements[113].

109 Article 12 de la directive.
110 Cette obligation aura donc des implications importantes pour le secteur du marketing direct. La personne concernée qui reçoit un mailing d'une entreprise devra être renseignée sur l'identité du prestataire ayant confectionné les listes d'adresses. Ce dernier, questionné par la personne concernée, devra alors, le cas échéant, la renseigner sur ses sources d'approvisionnement. En Belgique notamment, où cette obligation n'existe pas encore, on remarque que c'est précisément la question de la source des données qui préoccupe souvent les personnes concernées par les données.
111 Ces droits sont reconnus à l'article 8, b et c, de la Convention n° 108.
112 Il est à noter que l'article 12, § 3, de la loi belge prévoit que le maître du fichier doit communiquer les rectifications ou suppressions de données effectuées aux personnes auxquelles les données inexactes, incomplètes ou non pertinentes ont été communiquées, et ce pour autant qu'il connaisse encore les destinataires de cette information.
113 La réponse à cette question devra être envisagée au cas par cas. Si, par exemple, le destinataire des données vient à connaître le caractère inexact d'une des données traitées, il commettrait une négligence fautive en ne corrigeant pas celle-ci. Par contre, le verrouillage suite à l'inexistence de mesures de sécurité adéquates dans le chef du communiquant n'aura normalement aucune conséquence de ce type.

III. Exceptions communes

56. L'article 13 de la directive autorise les États membres à limiter certaines obligations (principe de finalité légitime, droit d'information, droit d'accès) lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention et la poursuite d'infractions pénales, l'intérêt économique ou financier d'un État membre ou de l'Union européenne, et la protection de la personne concernée ou des droits et libertés d'autrui[114].

Cette liste correspond aux buts énumérés à l'article 8, § 2, de la Convention européenne des droits de l'homme, au nom desquels une atteinte à la vie privée des individus est admise. Selon l'article 8, § 2, de la Convention, une atteinte à la vie privée est justifiée si elle poursuit l'une de ces fins et est en outre strictement nécessaire dans une société démocratique, c'est-à-dire si elle est pertinente, suffisante et proportionnée au but légitime poursuivi[115]. A cet égard, l'article 13 soulève une question particulière car, en admettant explicitement que des données à caractère personnel soient traitées en dérogeant à l'exigence de finalité légitime (article 6, *b,* de la directive[116]), cette disposition ouvre la porte à des hypothèses dans lesquelles l'application du principe de proportionnalité pourrait être éludée.

57. La portée exacte de l'article 13 de la directive dépendra en grande partie de ce que les États membres entendent par « la sûreté de l'État, la défense, (. . .) la protection des droits de la personne concernée ou des droits et libertés d'autrui ».

Le considérant 42 de la directive précise à cet égard que « les États membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les libertés d'autrui, limiter les droits d'accès et d'information ; ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut s'exerce sans l'intermédiaire d'un professionnel de la santé ».

58. L'article 13, § 2, évoque, par ailleurs, la possibilité pour les États membres de limiter par des mesures législatives les droits prévus à l'article 12 (à savoir le droit d'accès et de rectification) lorsque les données sont traitées exclusivement à des fins de recherche scientifique ou de statistiques. Cette possibilité doit s'accompagner de l'adoption par les États membres de « garanties »[117]. Il est toutefois exclu que les données puissent être utilisées dans ces cas aux fins de mesures ou de décisions se rapportant à des personnes précises.

Ainsi, on pourrait imaginer que dans le cadre d'essais cliniques de médicaments, un État membre permette de ne pas communiquer les données à la personne concernée afin qu'elle ne puisse savoir si elle est véritablement sous médication ou sous placebo. Il en va de la crédibilité même de la recherche. Toutefois, cette limitation du droit d'accès devrait être limitée à la durée de la recherche effectuée à propos de la personne concernée.

114 Voy. l'article 9 de la Convention n° 108 qui autorise également des dérogations aux obligations relatives à la qualité des données, aux traitement de données sensibles et aux droits de la personne concernée lorsque de telles dérogations constituent une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État, à la répression des infractions pénales ou à la protection de la personne concernée et des droits et libertés d'autrui.

115 Cf. supra, n° 29.

116 Cf. supra, n° 28 où il est démontré que l'article 6, b, de la directive consacre le principe de proportionnalité.

117 Voy. à ce sujet, la loi française n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O., 2 juillet 1994, 9559.

IV. Le droit d'opposition

59. L'article 14 de la directive reconnaît explicitement le droit pour la personne concernée de s'opposer pour des raisons prépondérantes et légitimes tenant à sa situation particulière à ce que des données la concernant fassent l'objet d'un traitement[118]. Si ce droit consacre *a priori* le droit pour tout individu de participer activement à l'utilisation de ses données, il convient toutefois d'en relativiser la portée. D'une part, libre cours est laissé aux États membres de prévoir des dispositions nationales contraires réduisant ou supprimant tout simplement ce droit[119]. D'autre part, afin de pouvoir s'opposer au traitement de ses données, la personne concernée doit invoquer des raisons « prépondérantes et légitimes tenant à sa situation particulière »[120]. Enfin, le droit d'opposition consacré par la directive ne revêt pas un caractère général. La personne concernée ne peut, en effet, s'opposer au traitement en lui-même mais uniquement au traitement de certaines données[121].

L'article 14 prévoit que le droit d'opposition doit exister au moins dans les cas visés à l'article 7, points *e* et *f,* de la directive. Ce droit peut s'entendre comme une compensation de l'article 7, *f,* qui autorise le traitement de données au nom d'un intérêt légitime du responsable ou d'un tiers, pourvu que l'intérêt du sujet des données ne prévale pas. Même si un État membre refuse d'accorder un droit d'opposition pour la personne concernée[122], cette dernière pourra néanmoins contester la balance des intérêts sur base de l'article 7, *f.* Ce faisant elle s'opposera au traitement de ses données à caractère personnel en arguant d'un intérêt prépondérant et légitime, ce qui est cependant plus exigeant que ce que prévoit l'article 14, *a* (avancer une *raison* légitime prépondérante tenant à sa situation particulière).

60. L'article 14, *b,* consacre en outre un droit général et inconditionnel d'opposition dans le cadre du traitement de données à caractère personnel à des fins de prospection[123]. Dans ce cas, la personne concernée ne doit plus apporter la preuve d'une raison légitime afin de s'opposer au traitement de ses données. La directive opère à cet égard une distinction entre deux hypothèses :

- soit le responsable du traitement effectue lui-même une action de prospection ; il doit alors offrir la possibilité pour la personne concernée de s'opposer gratuitement au traitement ;

118 Ce droit n'est pas prévu dans la Convention du Conseil de l'Europe qui n'accorde à la personne concernée que le droit de demander l'effacement des données en cas de manquement aux articles 5 (qualité des données) ou 6 (principes régissant le traitement de catégories particulières de données). Par contre, la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (J.O., 7 janvier 1978), prévoit en son article 26 que « toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'onjet d'un traitement ».

119 L'on pourrait imaginer qu'un État membre ne reconnaisse pas ce droit lorsque la personne concernée a donné son consentement indubitable au traitement en question.

120 La raison légitime ne doit pas, selon nous, être confondue avec l'existence ou non d'un fondement légitime au traitement des données trouvé dans l'article 7. Voy. contra. *P. Mei,* « The EC Proposed Data Protection Law », Law and Policy in International Business, vol. 25, 1993-1994, p. 316. Le critère retenu équivaut à une balance des intérêts à réaliser au niveau de l'individu.

121 Article 14 de la directive: « En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne pourra plus porter sur ces données ».

122 Voy. supra, « sauf disposition nationale contraire ».

123 La directive ne précise pas que cette prospection doit être de nature commerciale, ainsi la prospection pour une œuvre caritative ou un parti politique tombe sous le champ de l'article 14 (voy. Exposé des motifs, COM [92] 422 final – SYN 287, p. 27).

soit les données sont traitées à des fin de prospection, non pas pour le compte du responsable lui-même mais pour le compte d'un tiers auquel les données sont éventuellement communiquées. Dans ce cas, le responsable est tenu d'informer la personne concernée et de lui offrir un droit de s'opposer gratuitement à ladite communication ou utilisation et ce avant même la communication au tiers ou l'utilisation des données par ce dernier.

V. Décisions individuelles automatisées

61. L'article 15 stipule que les États membres doivent prévoir le droit pour toute personne « de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. ». Cette disposition vise donc à protéger la personne concernée contre le risque d'une utilisation abusive de l'informatique dans la prise de décision : « Le résultat fourni par la machine qui recourt à des logiciels de plus en plus sophistiqués, voire des systèmes experts, revêt un caractère apparemment objectif et incontestable auquel le décideur humain peut accorder une importance excessive, en abdiquant sa responsabilité »[124].

Trois conditions doivent être remplies afin de pouvoir invoquer l'article 15 :

- premièrement, il doit y avoir un traitement tendant à une décision produisant des effets juridiques à l'égard de l'individu ou l'affectant de manière significative ;
- deuxièmement, la décision doit être prise sur « le seul fondement d'un traitement automatisé ». Lorsque le processus de prise de décision contient une intervention humaine, l'article 15 ne pourrait être invoqué ;
- troisièmement, le traitement automatisé de données doit être destiné à évaluer certains aspects de la personnalité de la personne concernée. Une décision qui n'a pas pour objet l'évaluation de la personnalité d'un individu déterminé ne tombe dès lors pas sous le coup de l'interdiction (le processus de décision d'autorisation de retrait d'argent d'un distributeur automatique, sur base du solde du compte, par exemple).

Les États membres peuvent néanmoins prévoir qu'une personne peut être soumise à une décision individuelle automatisée soit lorsque cette décision est prévue par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée ; soit lorsque cette décision est prise dans le cadre d'un contrat, à la condition que la demande de conclusion ou d'exécution du contrat ait été satisfaite ou que des mesures appropriées (telles que la possibilité pour la personne concernée de faire valoir son point de vue) garantissent la sauvegarde de l'intérêt légitime de la personne. Dans le cas d'une telle décision, l'article 12 de la directive prévoit que la personne concernée doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui soustend le traitement automatisé de données la concernant.

124 Exposé des motifs, COM (92) 422 final – SYN 287, p. 27

VI. La notification

62. La directive établit en son article 18, § 1, le principe de la notification à adresser à l'autorité de contrôle, préalablement à la mise en œuvre d'un traitement[125]. L'obligation édictée porte sur les traitements entièrement ou partiellement automatisés ou les ensembles de tels traitements ayant une même finalité ou des finalités liées.

En règle générale, les réglementations actuellement en vigueur dans les États membres ne précisent pas le type de contrôle effectué à la réception de la notification. En pratique, cette dernière est fréquemment envisagée comme une formalité de publicité et n'est nullement assimilée à un système d'autorisation. Le contrôle à sa réception est bien souvent formel (rubriques non complétées, cohérence globale, etc.[126]) et n'empêche pas la mise en œuvre d'un traitement. L'examen de la licéité des traitements se situe plutôt *a posteriori,* sur base de la mise en cause du responsable du traitement, notamment en cas de plaintes émanant de particuliers. Bien entendu, dans ce cas, la notification constitue un élément d'appréciation important.

L'article 20 de la directive s'oriente partiellement dans une direction différente. Il impose aux États membres d'identifier *a priori* les traitements susceptibles de présenter des risques particuliers et de soumettre ceux-ci, préalablement à leur mise en œuvre, à l'examen de l'autorité de contrôle[127] ou du détaché à la protection des données[128]. En instaurant de cette façon un système de détermination préalable des traitements, la directive limite fortement le contrôle *a priori*[129]. Si l'on peut se rallier à une telle restriction en ce qui concerne ce type d'examen lorsqu'il est effectué par l'autorité de contrôle[130], elle paraît nettement plus contestable pour le détaché à la protection des données. En effet, c'est avant la mise en œuvre d'un traitement que la discussion la plus féconde peut avoir lieu. Dès lors que les traitements sont mis en œuvre, il est souvent délicat de les remettre en cause pour y intégrer des préoccupations de protection des données. A ce stade, la discussion est nécessairement plus polémique dans la mesure où des investissements importants peuvent avoir été réalisés et les pratiques déjà ancrées dans les mentalités des utilisateurs.

63. L'article 19 de la directive précise le contenu minimum de la notification. Cette dernière, envisagée comme un descriptif général, ne doit pas nécessairement faire apparaître tous les détails concrets du traitement, mais identifier le responsable du traite-

125 Selon le considérant 48, cette obligation a pour objet d'organiser la publicité des finalités des traitements en vue de leur contrôle. A noter que bien que la Convention n° 108 ne contienne pas de disposition en ce sens, de nombreuses législations nationales ont mis en place des systèmes de notification des traitements de données (Autriche, Danemark, Espagne, Grand-Duché de Luxembourg, Portugal, Royaume-Uni, etc.).

126 Voir la condamnation de la CNIL française pour refus de délivrance d'un accusé de réception (C.E. fr., 6 janvier 1997, Caisse d'épargne Rhône-Alpes Lyon, A.J.D.A., 1997, n° 2, p. 206).

127 Selon le considérant 54, la portée de l'intervention de l'autorité de contrôle devrait varier en fonction du droit national et prendre la forme soit d'une autorisation, soit d'un avis.

128 L'article 20, § 3, de la directive précise qu'« en cas de doute », le détaché à la protection des données consultera l'autorité de contrôle.

129 L'article 20, § 3, de la directive envisage un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées. Le considérant 53 mentionne diverses raisons pour lesquelles certains traitements pourraient présenter des risques particuliers, à savoir : leur nature, leur portée ou leur finalité, l'usage particulier d'une technologie. On peut penser, par exemple, à des traitements mis en œuvre par les pouvoirs publics et portant sur la totalité ou sur une proportion importante de la population ou à des traitements de données médicales. A noter que le considérant 54 laisse entendre que le nombre de traitements visés serait faible par rapport à l'ensemble de ceux qui sont mis en œuvre dans la société.

130 Un examen préalable systématique ne conduirait, en effet, qu'à créer un système administratif extrêmement lourd qui s'accompagnerait inévitablement de délais d'attente avant la mise en œuvre de traitements (cfr infra).

ment, la ou les finalités de celui-ci[131], indiquer les (catégories de) personnes et de données concernées ainsi que les destinataires[132], et enfin les transferts vers les pays tiers et les mesures de sécurité adoptées. Afin d'assurer la publicité des notifications, l'article 21, § 2, prévoit la mise en place d'un registre accessible au public et reprenant l'ensemble des notifications introduites auprès de l'autorité de contrôle[133].

64. De larges dérogations au principe de la notification obligatoire sont prévues, que ce soit sous forme d'exemption pure et simple ou de notification simplifiée[134]. Sur ce point, la directive laisse une grande autonomie aux États membres, tant en ce qui concerne la détermination des catégories de traitement qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes, que la possibilité de prévoir dans le droit national la désignation, par le responsable du traitement, d'un détaché à la protection des personnes chargé de garantir que les traitements concernés sont exempts de dangers[135].

La désignation d'un détaché à la protection des données agissant « en toute indépendance », paraît fort séduisante. Elle permettra d'échapper à la lourdeur administrative du système de notification[136], tout en garantissant la mise en œuvre de la législation au sein des organismes concernés. L'expérience allemande[137] en la matière s'est révélée

131 Voy. supra, point 15 en ce qui concerne la finalité comme critère de distinction des traitements. L'importance de la détermination de la finalité au moment de l'introduction de la notification ne doit cependant pas être sous-estimée car, en pratique, le responsable du traitement aura tendance à appliquer le principe de finalité sur base de celle-ci. L'expérience acquise au sein des États membres à cet égard montre que les responsables du traitement s'orientent généralement vers une description générique de la finalité. Dans ce cas, le contrôle peut difficilement s'exercer au regard du but global présenté, mais bien au regard des opérations particulières. Ainsi, pour un traitement défini sur base d'une finalité de gestion du personnel, on pourrait accepter l'emploi de données médicales en vue de la participation au remboursement de soins par l'employeur, mais leur utilisation pour d'autres objectifs spécifiques s'intégrant dans la finalité définie en termes larges (par exemple comme critère pour accorder ou non une promotion) doit être mise en cause.

132 À comparer avec l'article 1, § 4, de la recommandation R (87) 15 du Conseil de l'Europe relative aux données de police qui précise que la nature du fichier, l'organe responsable du traitement, les finalités de ce dernier, le type de données contenues et les destinataires auxquels les données sont communiquées doivent être déclarés.

133 Certains pays, comme le Royaume-Uni et la Belgique, envisagent la mise à disposition de ce registre public sur Internet.

134 La directive permet également aux États de prévoir une dérogation ou une simplification de l'obligation en faveur des traitements visés à l'article 8, § 2, d. Par ailleurs, en l'état actuel, différents pays ont déjà mis en place des systèmes permettant d'alléger les formalités de notification. Ainsi, la Belgique et les Pays-Bas ont soustrait à cette obligation bon nombre de traitements supposés moins risqués. La France a opté pour le régime des déclarations simplifiées dans lequel le responsable du traitement s'engage à mettre en œuvre un traitement en respectant les normes simplifiées définies par l'autorité de contrôle.

135 Aux termes de l'article 18, § 2, le détaché à la protection des données sera notamment chargé d'assurer l'application interne des dispositions nationales et la tenue d'un registre des traitements effectués par le responsable du traitement. Cette dernière obligation s'apparente à ce que l'on retrouve à l'article 16, § 1, de la loi belge du 8 décembre 1992 qui impose au maître du fichier de rédiger un du traitement.

136 Censée assurer la transparence des traitements tant vis-à-vis du grand public (via le registre public) que des autorités de contrôle, la notification préalable constitue une formalité administrative particulièrement lourde dont l'intérêt en termes de protection des individus et en particulier la valeur informative, peut être sérieusement mis en doute. Son principal (et unique?) avantage est de devoir être adressée à une instance externe – l'autorité de contrôle. Elle constitue dès lors un incitant pour les responsables de traitement à se familiariser aux règles de protection de données, les amenant notamment à s'interroger sur la légitimité et la pertinence des traitements qu'ils mettent en œuvre. La notification peut également former l'occasion privilégiée de nouer un dialogue entre les responsables des traitements (ou leurs organisations sectorielles) et les autorités de contrôle.

137 Datenschutzbeauftragter ou «DSB» très répandu tant dans le secteur privé où sa désignation est obligatoire que dans le secteur public où elle ne l'est pas toujours. Le délégué à la protection des données bénéficie, en vertu de l'article 36 de la loi fédérale allemande du 20 décembre 1990, d'une protection particulière tendant à renforcer l'efficacité de la fonction. En particulier, dans l'exercice de ses compétences en matière de protection des données, il ne reçoit d'instructions de personne. Il ne peut être désavantagé en raison de l'accomplissement de sa mission. L'organisation à laquelle il appartient doit l'assister dans l'accomplissement de sa mission et lui garantir l'accès nécessaire aux dossiers. Il est soumis au secret professionnel.

très positive. Le détaché constitue un interlocuteur privilégié entre les organismes qui doivent mettre en œuvre la législation de protection des données et la ou les autorités qui en assurent le contrôle. Dans la mesure où il agit au sein même de l'institution, il est en mesure de veiller en connaissance de cause à la mise en pratique de la protection[138]. Ce faisant, il contribue fortement à l'intégration des règles par ceux qui sont censés les mettre en œuvre et complète de la sorte la tâche de l'autorité de contrôle. Enfin, il constitue, de par sa proximité, un interlocuteur facilement accessible pour les personnes concernées souhaitant faire valoir leurs droits. Il apparaît cependant essentiel pour qu'il puisse agir de cette manière que la législation nationale fixe son statut afin de garantir au mieux son indépendance[139].

VII. La confidentialité et la sécurité des traitements

65. En vertu de l'article 17, § 1, de la directive, le maître du traitement a l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données[140]. Parmi les mesures techniques, on distingue les mesures de type physique, qui visent à protéger le système de la destruction par le feu, le gel, les pannes de courant, etc., des mesures de sécurité logiques, qui permettent de mettre en œuvre les principes de base de la protection des données[141].

Elles doivent permettre notamment que la collecte des données soit limitée aux données nécessaires, comme requis par l'article 6, *c,* de la directive, en empêchant que l'anonymat de la personne concernée ne soit levé sans nécessité[142]. Elles doivent également permettre que les données ne soient pas utilisées pour des finalités incompatibles, comme requis par l'article 6, *b,* en empêchant l'accès non autorisé aux données, ainsi que la lecture de celles-ci[143]. Elles doivent enfin permettre de garantir la fiabilité des données requise par l'article 6, *d,* en empêchant toute modification non autorisée des données.

A côté des mesures de sécurité techniques, les mesures de sécurité organisationnelles ou structurelles visent notamment à conscientiser le personnel au problème de la sécurité[144]. Parmi ce type de mesures, on mentionnera la nomination d'un détaché à la protection des données.

66. L'article 17, alinéa 2, de la directive prévoit que ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la

138 Le 49e considérant précise que le détaché peut être ou non employé par le responsable du traitement.

139 On ne peut, en effet, totalement exclure le risque que les caractéristiques du détaché à la protection et notamment son appartenance à l'institution où les traitements sont mis en œuvre ne lui permettent pas de réaliser sa tâche en toute indépendance.

140 L'article 7 de la Convention n° 108 prévoit une disposition similaire. Voy. aussi, pour des mesures de sécurité spécifiques, l'article 4 de la directive RNIS, précitée, l'article 8 de la recommandation R(87)15, précitée, concernant les données de police, l'article 13 de la recommandation R(89)2, précitée, relative aux données utilisées à des fins d'emploi, l'article 8 de la recommandation R(90)19, précitée, relative aux données utilisées à des fins de paiement, l'article 6 de la Recommandation R(95)4, précitée, relative aux données utilisées dans les télécommunications.

141 Voy. le commentaire de la recommandation R(97)19, précitée, l'article 126 de la Convention d'application de Schengen, et la recommandation R(97)5 du Conseil de l'Europe relative à la protection des données médicales, qui dressent une liste type des mesures de sécurité logiques.

142 Sur le principe de l'anonymat et les techniques des protecteurs d'identité (ou Privacy Enhancing Technology), cf. *J.-Ph. Walter,* « La protection des données à l'heure des inforoutes », Brig, Séminaire Multimédia du 25 avril 1997, organisé par l'Association suisse de révision interne, p. 9.

143 On vise ici les techniques de cryptage, de codage et de chiffrement. Il semble à l'heure actuelle qu'une clef de 128 bits offre un niveau de sécurité suffisant (idem).

144 Cfr point 72 de la recommandation R(90)19, précitée.

nature des données. Parmi les différents facteurs de risques relatifs aux données, on distinguera ceux relatifs aux données elles-mêmes (nature des données, nombre des données, nombre de personnes concernées, etc.), ceux concernant les finalités (nature de la finalité, multiplicité de finalités poursuivies par le traitement, finalité informative ou décisionnelle), ceux touchant à la nature de la relation juridique entre la personne concernée et le responsable du traitement, etc. Parmi les facteurs de risque relatifs au traitement, on mentionnera la structure interne du traitement, la multiplicité des utilisateurs, la multiplicité des localisations du traitement entraînant un accroissement des risques d'effraction (la localisation à un seul endroit augmentant, quant à elle, les risques liés à l'effraction), la technologie du traitement (les données contenues en réseau auquel chaque utilisateur peut accéder présentent plus de risques que celles traitées par un ordinateur personnel non connecté).

67. L'article 17 précise que les mesures doivent être adéquates au regard de l'état de l'art et de la technique[145]. C'est donc une conception nécessairement évolutive du niveau de sécurité qui est prônée, en relation avec l'évolution technologique dans le domaine.

La directive impose des obligations de sécurité supplémentaire aux responsables de traitement qui recourent à un sous-traitant : ils sont en effet tenus de choisir un sous-traitant qui apporte des garanties suffisantes du point de vue de la sécurité. En outre, le contrat qui les lie doit être rédigé par écrit et prévoir que le sous-traitant n'agit que sur instruction du responsable du traitement.

L'article 16 généralise ce dernier principe en disposant que toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant ne peut, sauf obligation légale contraire, traiter ces données que sur instruction du responsable du traitement[146].

E. Les flux transfrontières de données

68. Si la directive entend rechercher une équivalence de protection des données à caractère personnel dans les différents États membres, elle s'attache également à régler le problème du droit national applicable à la réalité réglementée. La détermination du droit applicable est particulièrement nécessaire eu égard au développement de la dimension de plus en plus internationale des traitements de données à caractère personnel.

Tant que les données ne quittent pas le territoire de la Communauté, les règles de détermination de la loi nationale applicable sont censées suffire pour sauvegarder le niveau de protection des personnes concernées. La difficulté est alors d'éviter que le régime protecteur soit réduit à néant dès que ces données sortent du territoire européen tant il est vrai que la dimension internationale des flux d'informations, y compris nominatives, rendrait vaine l'existence d'une réglementation dont l'effectivité couvrirait le seul territoire européen. Les autoroutes de l'information que préfigure la toile d'Internet favoriseront encore cette circulation sans frontières, qu'il s'agisse de flux liés à la mobilité des personnes, de flux liés à un commerce électronique croissant ou à la consultation de sites étrangers, de flux, enfin, liés à des transmissions à l'intérieur d'un groupe d'entreprises, d'un secteur ou intersectoriels.

145 Le paragraphe 117 de l'annexe de la recommandation R(97)5 précise que les mesures de sécurité devraient être à la hauteur des développements technologiques des systèmes d'information sans pour autant donner lieu à des dépenses démesurées. Comp. avec l'article 4, § 2, de la directive RNIS qui requiert que les mesures de sécurité soient prises « compte tenu des possibilités techniques les plus récentes ».

146 Ces deux dernières dispositions ont leur équivalent dans la Convention n° 108.

Les règles par lesquelles la directive tente de répondre à cette réalité font l'objet du commentaire qui suit. L'article 4, 1, *a*, permet de déterminer la loi nationale applicable et, par là, permet d'appréhender le régime des flux intracommunautaires de données (A). La directive assortit également de conditions les flux de données hors Europe (articles 25 et 26) et soumet, exceptionnellement, le responsable situé hors du territoire européen aux prescrits de la directive européenne (article 4, 1, *c*) (B)[147].

I. Les flux transfrontières intracommunautaires

69. Les auteurs de la directive sont partis du principe qu'un traitement ne devait normalement être soumis qu'à l'application d'une seule législation nationale[148].

Le critère de la localisation physique du traitement, retenu à l'origine, a été détrôné par celui du lieu de l'établissement du responsable du traitement. Vu la dimension internationale des traitements, ceux-ci auraient en effet été localisés dans chacun des États où une opération particulière était effectuée.

Le principe est énoncé à l'article 4, 1, *a*, de la directive. Si un traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement, la loi nationale applicable est celle du lieu où cet établissement est situé. L'établissement sur le territoire d'un État membre « suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable »[149]. La forme juridique retenue n'est donc pas déterminante : simple succursale, filiale ayant la personnalité juridique, etc.

70. On peut se demander si le critère retenu permettra toujours d'éviter une application de plusieurs législations au même traitement. Un cas simple est celui où plusieurs sociétés distinctes, établies sur des territoires différents, décident de créer un traitement commun : elles sont chacune considérées comme responsables du traitement. En application de la règle générale, chacune de leur loi nationale s'applique au traitement en cause.

Le responsable du traitement peut avoir différents établissements stables sur le territoire européen. Dans ce cas, la même disposition énonce qu'il « doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ». La justification de cette solution semble être à trouver d'une part dans l'idée d'application de la loi la plus proche de la personne concernée, ce qui devrait permettre à cette dernière de demander l'application de la loi qu'elle connaît le mieux et pour laquelle elle est le mieux armée à en exiger l'application et d'autre part, dans la volonté d'éviter un contournement de législation[150].

Ici encore, on en arrivera à une application possible de plusieurs lois nationales au même traitement. On pense au cas où un traitement centralisé en un lieu déterminé dessert différentes sociétés d'un même groupe délocalisé sur plusieurs États membres.

En toute hypothèse, les solutions pourront encore être rendues plus complexes dès lors que des États interprètent différemment les notions de traitement ou de responsable, intervenant dans la mise en œuvre du critère de rattachement.

71. Si seules des lois nationales des États membres sont applicables aux traitements en cause, aucune difficulté ne devrait plus survenir lors de flux transfrontières de données intracommunautaires. En effet, le principe inscrit à l'article 1, 2, de la directive interdit toute restriction ou interdiction apportée à la libre circulation des données au nom de sa loi nationale.

147 Nous reviendrons infra sur la combinaison de ces différents articles.

148 Exposé des motifs, précité, p. 12.

149 Voy. considérant n° 19.

150 Voy. considérant n° 19.

C'est peut-être oublier le problème de la marge de manœuvre laissée aux États membres dans la confection de leur législation nationale. En effet, on a vu que le principe de l'article 1, 2, était fondé sur l'idée de l'existence d'une protection équivalente dans les différents États membres du fait du rapprochement des législations nationales prises en conformité avec la directive. Vu la large marge de manœuvre laissée à ceux-ci à de nombreux niveaux de la protection, des traitements seront interdits par certains États et permis par d'autres. Par exemple, la Belgique interdit le traitement d'un certain type de données sensibles sauf si l'on obtient le consentement de la personne concernée alors que les Pays-Bas conservent l'interdiction complète de traitement en application de l'article 8, 2, *a.* Il s'agit assurément d'un cas de disparité entre législations nationales permise par la directive. Si une société établie en Belgique veut commercialiser ces données aux Pays-Bas, ses clients potentiels qui y sont établis devront refuser le transfert sous peine d'être en infraction avec leur propre loi nationale : la collecte de telles données y est illicite. Ce faisant, les Pays-Bas restreignent la libre circulation des données entre deux États membres. On touche là à une contradiction essentielle trouvant sa source dans la directive elle-même. Dans l'exemple précité, les Pays-Bas respectent le prescrit de la directive concernant les données sensibles. La société belge peut par contre en appeler à l'article 1, 2, pour exiger que le flux de données envisagé soit autorisé.

Deux interprétations sont alors permises. La première consiste à admettre que les divergences entre les législations nationales, dans la mesure où elles se situent dans les limites de la marge de manœuvre laissée aux États membres, participent néanmoins à un niveau de protection équivalent de sorte que le refus du flux soit interdit. Pour que ce principe conserve une véritable portée, il faut alors admettre que le destinataire des données puisse continuer à traiter les données reçues nonobstant la règle contenue dans sa loi nationale. L'exigence de protection serait donc toujours équivalente à celle contenue dans la loi nationale la plus laxiste. L'autre consiste à admettre le refus du flux comme exception à l'article 2, 1, dès lors que sa *ratio* n'est pas respectée, mais c'est alors aller au-delà du texte de cette disposition. On peut gager que cette difficulté devra impérativement trouver une solution rapide au niveau communautaire sauf à enlever une grande portée au résultat de l'adoption de la directive commentée.

II. Les flux transfrontières vers des pays tiers

1. Le principe : la nécessité d'une protection adéquate[151]

72. En vertu de l'article 25, 1, de la directive, « les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel, faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat ». Le principe est donc l'interdiction du transfert sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25, 2, que l'appréciation[152] du caractère adéquat de la protection du pays tiers doit tenir compte de « toutes les circonstances relatives à un transfert ou à une catégorie de transferts » et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et d'autres concernent le niveau de protection dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

151 Sur l'étude de cette notion, voy. *Y. Poullet, B. Havelange,* (avec la collaboration de *M.-H. Boulanger, H. Burkert, C. de Terwangne, A. Lefebvre*), Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel, Exec. Summary, Étude réalisée pour la Commission européenne, février 1997, à paraître.

152 Le texte ne précise pas de qui relèvera l'appréciation du caractère adéquat ni quel rôle l'autorité de contrôle jouera dans cette procédure.

73. Le texte de l'article 25 suggère une triple approche de la notion de « protection adéquate » :

- *une approche au cas par cas*[153], c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée « par rapport à un transfert déterminé ou une catégorie de transferts » ;
- *une approche souple et ouverte* puisque selon le libellé même de l'article 25, 2, l'évaluation doit pouvoir tenir compte à la fois des particularités propres des divers flux transfrontières mais également des solutions diverses et évolutives que chaque État, voire chaque responsable des données, peut apporter, l'article 25, § 2, étant purement indicatif à ce propos ;
- *une approche fonctionnelle,* c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

L'évaluation de ces mesures doit se faire sans *a priori;* il ne peut être question d'imposer les mécanismes européens mis en place en application de la directive (pas d'impérialisme européen), mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non, par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données telle qu'organisée par la directive. En effet, la notion de protection adéquate induit la confrontation des exigences de protection de la directive avec les réponses données par les pays tiers. Il s'agit de rechercher s'il y a « similarité fonctionnelle ». La « similarité fonctionnelle » implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si lesdits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité législative complète[154].

74. Quelques éclaircissements s'imposent encore au sujet de la notion d'« adéquation ».

Tout d'abord, cette notion suppose un référent permettant de répondre à la question : « Par rapport à quoi la protection doit elle être adéquate » ? Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par

153 Par opposition à une approche légistique qui se fonderait sur la seule comparaison des textes en vigueur dans le pays tiers par rapport à la directive.

154 La notion de protection équivalente est utilisée par la Convention n° 108 du Conseil de l'Europe en son article 12. Cet article met à charge d'une partie contractante une obligation de permettre les flux de données sensibles vers les autres États parties à la Convention qui assurent une protection équivalente à celle de l'État émetteur. On notera que la notion d'équivalence de protection ne règle que les flux entre pays ayant ratifié la Convention du Conseil de l'Europe et non vers les pays tiers. A propos de cette différence, voy. *A. Bourlond, Y. Poullet,* « Flux transfrontières de données à caractère personnel, position de la proposition de directive européenne face à celle de la convention 108 du Conseil de l'Europe », D.I.T., 1991/2, p. 58 et s.

rapport auquel on puisse évaluer la protection du pays tiers. Sans doute faut-il considérer qu'il s'agit des principes de base de la directive, sans s'arrêter à la forme ou aux modalités particulières attachées à ces principes dans le texte européen.

Ensuite, on note que, si les critères énoncés par l'article 25, 2, constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive[155]. On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

Troisièmement, le contenu de ces éléments n'est pas défini: si, par exemple, on sait qu'il faut prendre en compte la durée des traitements, la directive ne précise pas ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devrait être le « contenu minimum » d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection[156].

Enfin, à propos des instruments de protection mis en place dans le pays tiers, l'article 25 se réfère non seulement aux normes issues de l'autorité publique, qu'elles soient générales ou sectorielles[157], mais également aux codes de conduite[158] voire aux mesures techniques, pourvu que ces instruments soient respectés. Ainsi, la personne chargée d'évaluer la protection étrangère sera plus attentive à l'« effectivité » d'un instrument qu'à sa nature : ce qui importe, c'est que la connaissance de l'instrument, même s'il s'agit d'une simple *company privacy policy,* soit largement répandue parmi les personnes concernées et les responsables des fichiers; de même, on sera attentif à la possibilité d'un recours des particuliers à l'encontre des responsables de fichiers en cas de non-respect des instruments en question.

75. L'article 25, alinéas 1 et 2, consacre, nous l'avons dit, une approche au cas par cas, flux par flux, ou catégorie de flux par catégorie de flux. Une telle démarche est évidemment lourde pour les États membres, aussi les articles 25, 4, et 25, 6, ouvrent deux voies d'allégement de la tâche par le biais de la Commission. Il s'agit de constater, conformément à la procédure prévue à l'article 31, § 2, « qu'un pays tiers assure ou n'assure pas un niveau de protection adéquat ». En d'autres termes, ces paragraphes permettent la constitution de *white* ou de *black lists,* décision valable pour des catégories de transferts, pour un secteur voire pour l'ensemble des flux vers un pays tiers[159].

155 L'article 25, 2, énonce qu'il faut « en particulier » prendre en considération tel ou tel élément.

156 A cet égard, l'article 25, § 6, dispose qu'un pays tiers peut être considéré comme assurant un niveau de protection adéquat « en raison de ses engagements internationaux ». La question se pose de savoir s'il faut considérer sur base de cette disposition qu'un État tiers, partie contractante à la Convention n° 108, offre un niveau de protection adéquat. Une réponse positive signifie qu'en présence de flux transfrontières la directive n'offre pas un niveau de protection plus élevé que la Convention n° 108. En cas de réponse négative, les États membres de l'Union qui sont également parties à la Convention peuvent être pris dans une situation inextricable. En vertu de la directive, ils ne pourront autoriser certains flux, alors qu'en vertu de l'article 12, 2, de la Convention n° 108, ils ne pourront les empêcher (sauf concernant certaines données sensibles). A ce jour, seuls trois États sont parties contractantes à la Convention sans être membres de l'Union: la Slovénie, la Norvège, l'Islande.

157 Ainsi, une législation sur le secret médical pourrait garantir dans le secteur médical, la protection des données.

158 La Canadian Standard Association a établi un code de conduite modèle en matière de respect de la vie privée qui prévoit des mécanismes originaux de certification pour les entreprises par des organismes agréés et la possibilité de recours. A propos de ce modèle: *C. Bennett,* Privacy Codes, Privacy Standards and Privacy Laws: the instruments for Data Protection and what they can achieve, Paper presented at Visions for Privacy, Victoria, British Columbia, 9-11 mai, 1996.

159 Analyse au cas par cas et analyse globale : les deux types d'analyse ne sont pas contradictoires. L'analyse globale suivra le plus souvent une série d'évaluations au cas par cas, éventuellement pratiquées par différents États membres; elle pourrait également se déduire d'un système de protection générale des données dont le contenu, le contexte et l'application conduisent de façon évidente à la reconnaissance de l'adéquation ou l'inadéquation de la protection offerte.

76. En ce qui concerne les bénéficiaires de la protection adéquate, la directive se limite à protéger les données des personnes bénéficiant au départ de la protection de la directive lorsque ces données sont envoyées à l'étranger.

Par conséquent, ce que la directive impose, ce n'est pas une protection s'appliquant à l'ensemble de la population mondiale, mais plutôt la garantie aux personnes bénéficiant au départ de la protection de la directive, du maintien d'une protection adéquate pour les traitements même non soumis à la directive. Ainsi, le responsable étranger d'un traitement pourrait, sans modifier les règles de protection qu'il suit habituellement, réserver aux seules personnes originairement bénéficiaires de la protection européenne, la « protection adéquate » de l'article 25.

2. Les exceptions

77. La directive édicte certaines exceptions au principe de l'article 25, « sous réserve de dispositions contraires du droit national régissant des cas particuliers »[160]. De la sorte, des transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat peuvent avoir lieu en certaines circonstances. Deux types d'exception sont prévus: le premier tient compte du contexte dans lequel s'inscrit le flux; le second substitue un mode de protection *ad hoc,* à la protection adéquate : le contrat.

À propos de la première catégorie d'exceptions, l'article 26, 1, *a,* vise l'hypothèse où la personne concernée a indubitablement donné son consentement à l'opération de transfert. On ne peut parler de véritable consentement que si celui-ci est[161], c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, si elle connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données. D'autres exceptions existent. Elles concernent les transferts nécessaires à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles, soit entre la personne concernée et le responsable du traitement, soit entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée[162]. Sont également visés les transferts servant à la sauvegarde d'un intérêt vital ou d'intérêts publics importants, ou encore s'opérant dans le cadre d'une action en justice. L'article 26, 1, *f,* prévoit encore le cas des transferts à partir d'un registre public « destiné réglementairement à l'information du public et ouvert à la consultation » (ainsi, par exemple, le registre du commerce).

On notera qu'il importe que le transfert soit nécessaire au regard de tels intérêts et qu'il ne suffit pas que l'intérêt contractuel existe pour que le transfert soit autorisé[163]. Ainsi, dans le cadre d'une multinationale, la création en terre lointaine d'une banque de

160 « Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat (...) peut être effectué (...) » (article 26, 1). « Les États membres peuvent donc, pour des dispositions régissant des cas particuliers, refuser que l'une ou l'autre exception s'applique à ces cas. On pense dans un premier temps aux situations mettant en jeu des données sensibles, médicales ou judiciaires. Mais la particularité des cas retenus peut être plus large, et consister non plus dans le caractère sensible des données mais, par exemple, dans la nature d'un réseau – ouvert ou fermé – utilisé. On peut donc imaginer qu'un État membre soit plus strict qu'un autre en matière d'exceptions appliquées à l'utilisation d'un réseau Internet » autre en matière d'exceptions appliquées à l'utilisation d'un réseau Internet» *(M.-H. Boulanger, C. de Terwangne,* in *E. Montero (éd.),* Internet face au droit, Cahier du CRID n° 12, Bruxelles, Story-Scientia, 1997, p. 211). A côté de cette interprétation large, la notion de « cas particulier » pourrait toutefois s'envisager comme laissant la possibilité pour l'autorité nationale de n'intervenir que pour un flux déterminé et de ne déroger qu'exceptionnellement et non par catégorie aux différentes hypothèses prévues par l'article 26.

161 Sur cette notion, cf. supra.

162 Ainsi, par exemple un service de réservation aérienne transmettra à des agences locales de voyage, le nom des voyageurs désirant réserver un hôtel.

163 L'article 26 constituant une exception doit s'interpréter de manière stricte.

données relative à l'ensemble des travailleurs et les flux engendrés à partir des filiales européennes ne pourront bénéficier de l'exception de l'article 26 que si le responsable démontre qu'il existe une nécessité d'opérer ces transferts pour l'exécution du contrat.

La seconde catégorie d'exceptions vise des substituts fonctionnels à la protection adéquate élaborée par la directive. Les clauses contractuelles sont visées en particulier[164]. Ainsi, si le secteur marketing d'un pays tiers n'offre pas de protection adéquate aux données originairement protégées par la directive, une entreprise ou l'association des sociétés de marketing peut prendre dans le cadre des contrats couvrant les flux transfrontières en provenance d'Europe, des engagements supplémentaires, par exemple limitant les finalités de réutilisation des données, ouvrant le droit d'opposition et finalement permettant à une autorité de protection des données d'inspecter les traitements. A propos de ce second type d'exception, une autorisation de l'État membre est nécessaire[165]. L'accorder revient à reconnaître le caractère « suffisant » des garanties offertes. L'État membre doit informer la Commission de telles autorisations, des oppositions pouvant être exprimées par d'autres États membres. On souligne à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des États membres[166], inviter[167] les États membres à agir : soit à accepter de telles mesures palliatives, soit à les rejeter ou proposer des mesures supplémentaires.

III. L'applicabilité extraterritoriale de la directive

78. Selon l'article 4, 1, *c*, de la directive, le droit national pris en application de la directive s'applique « lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre ». L'article 4, 2, ajoute que l'applicabilité du droit national entraîne l'obligation pour le responsable de désigner un représentant établi sur le territoire de l'État membre[168].

Le critère de rattachement affirmé par le texte est donc le « recours » à des moyens, automatisés ou non, situés sur le territoire de l'Union européenne. La notion est vague. Prise au sens large, elle couvrirait les hypothèses où la collecte des informations, opérée par exemple en Belgique, est suivie d'un transfert des données vers l'étranger pour les y traiter à meilleur prix. Correspondrait aussi à recourir à des moyens situés en territoire

164 Des mesures techniques ad hoc pourraient également être envisagées. Sur les contrats comme moyen supplétif d'assurer une protection équivalente ou adéquate dans les flux transfrontières, voy. *C.M. Pitrat,* « Clauses modèles pour les flux transfrontières de données ou comment assurer une protection équivalente », D.I.T., 1993/1, pp. 46 à 52; *L. Early,* Securing equivalent protection among nations in the context of TBDF, D.I.T., 1990, n° 4, p. 10 et s. Le lecteur trouvera dans ces écrits des références aux clauses modèles élaborées conjointement par le Conseil de l'Europe, la Commission européenne et la CCI (Strasbourg, 2 nov. 92, T.PD[92] 7 revised). A noter que la recommandation R (89)2 sur la protection des données utilisées à des fins d'emploi envisage explicitement la possibilité de recourir au contrat pour garantir que le destinataire sis dans un pays tiers respecte les principes énoncés dans la recommandation (cf. Exposé des motifs, paragraphe 63).

165 Pour une critique judicieuse de ce modèle, lire l'article de *J. Reidenberg,* Setting Standards for Fair Information in the US. Private Sector, Iowa Law Review, March 1995, Volume 80/n° 3.

166 Il est à noter que dans ce cas, le groupe d'experts (reprenant des membres des autorités de protection nationales) ne joue pas de rôle explicite... La matière, on le pressent, est hautement politique.

167 Cette invitation devra, pour devenir décision, suivre la procédure de comitologie définie par la décision du Conseil du 13 juillet 1987, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission, J.O.C.E., 1987, n° L 197/34.

168 Comp. avec l'obligation imposée par l'article 1, § 6, de la loi belge à charge du maître du fichier situé à l'étranger de nommer un représentant auprès duquel les droits d'accès et de rectification s'exerceront. La même idée est poursuivie par la directive.

communautaire le fait d'interroger depuis l'extérieur de l'Union une banque de données sise en Belgique. L'applicabilité de la directive s'étendrait même à un système de réservation aérienne dans la mesure où c'est en interrogeant une boîte aux lettres tenue à sa disposition en Europe par une agence de voyages, que la personne désireuse d'opérer une réservation prend connaissance de messages EDI qui lui sont destinés.

Bref, l'interprétation large de la notion de « recours » aboutirait à décréter que la quasi-totalité des flux transfrontières amènerait le destinataire des flux à tomber sous le coup des dispositions de la directive. Point ne serait besoin alors des articles 25 et 26 de la directive, puisqu'en toute hypothèse cette dernière serait applicable.

Lors d'une analyse récente de l'application de la directive à Internet, une autre interprétation, qualifiée de téléologique –, du critère de rattachement défini par l'article 4, 1, *c*, a été proposée[169]. L'argumentation sous-tendant cette interprétation s'articule comme suit :

« La ratio legis de cet article se résume clairement dans la volonté d'éviter que les individus se trouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la directive, même en dehors des frontières communautaires ». C'est par une lecture combinée de l'article 4, 1, *c*, et des articles 25 et 26 qui régissent les flux transfrontières vers les États tiers qu'une définition rationnelle de l'applicabilité de la directive pourra être dégagée.

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communauté. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à l'étranger en provenance de l'Union. Une protection adéquate des données envoyées à l'étranger en provenance de l'Union est exigée.

La réponse contenue dans l'article 4, 1, *c*, vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés par une manœuvre artificielle du bénéfice de la protection de l'ensemble de la directive, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 4, 1, *c* :

- celle précisément où un responsable de traitement cherche délibérément à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire communautaire pour réaliser son traitement.
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. Il en est ainsi d'un logiciel qui permettrait à un responsable sis à l'étranger de visiter l'ensemble des forums de discussions mis en place par des serveurs européens et d'y repérer les interventions de telle ou telle personne afin de constituer son profil de personnalité.

En conclusion, l'article 4, 1, *c*, viserait des hypothèses exceptionnelles soit celle où la localisation du responsable est anormale au regard de son activité orientée vers l'Union européenne et portant sur des données en provenance de celle-ci, soit celle où est

169 *C. de Terwangne, S. Louveaux,* op. cit., p. 237 et s. et *M-H. Boulanger, C. de Terwangne,* op. cit., p. 202. Les auteurs se réfèrent également à la lecture du considérant 20 de la directive et à l'exposé des motifs de la première proposition de directive émanant du Conseil (proposition du 15 oct. 1992, COM(92) 422 final – SYN 287, p. 13).

déjouée la protection offerte par la réglementation des flux transfrontières dans la mesure où le flux est généré par la seule activité de la personne située à l'étranger sans qu'il y ait à proprement parler communication, c'est-à-dire action de transfert de données, d'un responsable de traitement situé dans le territoire de l'Union européenne.

F. Les codes de conduite

79. La directive prévoit que les États membres et la Commission « encouragent » l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales[170]. Les rédacteurs de tels codes pourront les soumettre aux autorités de contrôle qui en vérifieront la conformité au regard de la réglementation[171].

Le texte envisage également l'élaboration de codes communautaires qui peuvent, quant à eux, être soumis au groupe européen de protection des données[172] qui examinera notamment s'ils respectent les dispositions nationales[173].

Lorsque des codes seront soumis à leur approbation, tant l'autorité nationale de contrôle que le groupe européen pourront recueillir, s'ils l'estiment opportun, les observations des personnes concernées ou de leurs représentants. En outre, selon qu'il s'agira d'un code national ou communautaire, chacune de ces deux instances pourra respectivement en assurer la publicité.

80. L'adoption de codes de conduite en aval des réglementations nationales issues de la directive peut se révéler très positive lors de la mise en œuvre des normes protectrices. Émanant des secteurs eux-mêmes, ces codes sont en principe élaborés au niveau le plus approprié – celui où surgissent les problèmes – et sont dès lors en mesure d'énoncer des solutions adaptées aux réalités, traduisant de manière concrète les principes formulés en termes généraux dans les réglementations[174]. Au surplus, ils sont aisément modifiables, ce qui leur permet de suivre facilement les évolutions des secteurs. Un argument de type économique – censé jouer sur l'image du responsable du traitement – peut encore être relevé: les codes de conduite, pourraient, selon certains, améliorer la confiance de la personne concernée dans les services proposés par une entreprise qui s'y soumet volontairement. On soulignera enfin l'intérêt des codes communautaires qui devraient contribuer à réduire pour un même secteur les divergences entre les protections mises en place au sein de chaque État membre.

On ne peut toutefois passer sous silence certains de leurs inconvénients. Largement issus d'une démarche volontaire, la sanction de leur non-respect peut être difficile à mettre en œuvre[175]. À la limite, leur adoption peut servir d'alibi pour offrir une façade de

170 Article 27, § 1, de la directive. A noter que le paragraphe 39 du Rapport explicatif de la Convention n° 108 insiste également sur l'intérêt de mesures réglementaires volontaires, tels des « codes de bonne pratique ou des règles de conduite ». La recommandation R (85) 20 du Conseil de l'Europe relative aux données utilisées à des fins de marketing (précitée) va dans le même sens.

171 Article 27, § 2, de la directive. Par les mots « peuvent être soumis », la directive prévoit la possibilité de consulter l'autorité de contrôle, mais ne l'impose pas.

172 Cf. infra.

173 Cf. infra, le groupe institué par l'article 29 de la directive. L'examen au regard des dispositions nationales adoptées en application de la directive pourrait donner lieu à quelque difficultés dans la mesures où ces législations peuvent présenter des divergences significatives (cfr. supra). Quelle sera dès lors la référence en matière de codes communautaires ?

174 A moins, bien sûr, qu'il ne s'agisse d'un simple « recopiage » de ces principes.

175 Il existe de multiples variétés de codes de conduite. Le degré d'effectivité de chacun de ceux-ci s'évaluera en fonction de circonstances propres à leur adoption et à leur mise en œuvre. On notera, à titre d'exemple, le pouvoir des organismes ou fédérations sectorielles vis-à-vis de leurs membres, l'existence de mécanismes de suivi, la portée concrète de leurs dispositions ou encore la publicité qui leur est donnée.

respectabilité aux organismes concernés. Certes, rien n'empêche les États de leur reconnaître une valeur réglementaire ou de prévoir des procédures d'homologation officielle. Toutefois, cette démarche se heurte souvent au problème de la représentativité des instances à la base des codes.

Les codes ne sont pas non plus soumis à une publicité organisée et ne tiennent compte que dans une certaine mesure de l'intérêt des personnes concernées. En effet, même si leurs rédacteurs sont souvent conscients de la nécessité d'assurer une protection de ces dernières, ils la transposent dans leur logique propre, généralement sans que n'existe de réel débat permettant d'assurer une juste mise en balance des intérêts en présence.

Par ailleurs, l'élaboration de ces codes de conduite n'est pas chose aisée dans la mesure où traduire les dispositions à caractère général des réglementations de protection des données en mesures spécifiques, peut donner lieu à des interprétations divergentes. On doit cependant relever que pareille démarche constitue souvent l'occasion d'une prise de conscience des enjeux de la protection des données de même que l'occasion de nouer un dialogue productif entre les milieux professionnels et les autorités de contrôle.

En tout état de cause, les codes de bonne conduite n'exemptent pas les secteurs de l'application des législations nationales issues de la directive qui garantiront, en termes généraux certes, le respect des droits subjectifs et les possibilités de recours des personnes concernées[176]. Cette soumission à la loi, en définitive, apporte aux codes sectoriels, ne fût-ce qu'indirectement, une effectivité certaine étant donné que la loi s'accompagne de force juridique contraignante qui reste l'ultime garantie de l'efficacité des principes énoncés.

G. Les organes de contrôle

I. Le contrôle au niveau national

81. Confirmant l'approche retenue dans les législations nationales issues de la Convention du Conseil de l'Europe[177], la directive impose à chaque État membre d'instituer en son sein une ou plusieurs autorités publiques, chargées de surveiller l'application des réglementations édictées. Elle énonce, en outre, les grands principes régissant la mise en place de ce type d'autorités, mais laisse toutefois aux États membres la liberté de décider de l'opportunité d'en établir une ou plusieurs[178] et d'en déterminer exactement la « physionomie ».

176 De manière similaire, le paragraphe 39 du Rapport explicatif de la Convention n° 108 ne les envisage qu'en tant que complément utile à des mesures de type contraignant (lois, règlements, directives administratives, etc.) et insiste sur le fait que de telles mesures « ne suffisent pas par elles-mêmes pour donner suite à la convention ».

177 A titre d'exemple, en France, la Commission nationale de l'informatique et des libertés (CNIL), en Belgique, la Commission de la protection de la vie privée, en Allemagne, le délégué fédéral à la protection des données élu par le Bundestag et compétent pour les traitements des organismes publics fédéraux et pour le secteur privé, et par ailleurs des autorités de contrôle désignées par les Länder, et aux Pays-Bas, la Registratiekamer. A noter que la Convention n° 108 ne prévoit pas l'institution d'autorités de contrôle, mais bien celle d'autorités destinées à favoriser la coopération entre les États signataires. Par contre, la recommandations R (87) 15 relative aux données de police (précitée) suggère explicitement la mise en place d'autorités de contrôle.

178 Les États membres sont libres d'opter pour une seule autorité chargée de l'ensemble des questions de protection des données ou pour plusieurs autorités exerçant leurs activités dans des domaines spécifiques. On doit souligner que la deuxième solution implique la mise en œuvre de procédures efficaces permettant aux diverses autorités d'agir de manière concertée.

Les autorités de contrôle sont supposées exercer en toute indépendance les missions dont elles sont investie[179]. Il s'agit là d'une de leurs caractéristiques fondamentales censée permettre qu'émergent des solutions équilibrées tenant compte des divers intérêts en présence. Cette caractéristique se reflétera, par exemple, dans le fait que les autorités ne sont pas intégrées dans une hiérarchie administrative classique, qu'elles jouissent d'une autonomie budgétaire, que leurs membres ne peuvent être relevés de leurs fonctions, que des mesures d'incompatibilité frappant ceux-ci sont édictées, que leur composition garantit une pluralité d'opinions et assure une certaine représentativité des personnes concernées. En pratique, l'indépendance peut pourtant se révéler une véritable gageure. En effet, d'un côté, la composition des autorités révèle souvent l'empreinte des pouvoirs politiques en place, ce qui peut freiner la mission protectrice des organes lorsque des mesures contestables sont adoptées par les gouvernants[180], et de l'autre côté, certaines autorités peuvent être tentées de défendre d'une manière paraissant excessive les droits et libertés des individus, mettant de la sorte en jeu leur crédibilité.

82. La directive entérine les approches nationales en termes de missions et de pouvoirs dévolus aux autorités de contrôle. De manière générale, ces dernières seront chargées de la surveillance de l'application de la réglementation. Pratiquement, on peut, pour l'essentiel, mettre en évidence trois formes d'interventions. Premièrement, elles ont un rôle de conseil à l'égard du pouvoir réglementaire. La directive n'impose cependant pas que les avis émis soient conformes[181]. Deuxièmement, les autorités tendent à « éveiller les consciences » non seulement en informant le public de la portée des droits et obligations résultant de la législation, mais également en assurant une certaine publicité aux prises de position portant sur des questions particulières[182]. Troisièmement, elles interviennent en tant qu'arbitre dans les conflits entre ficheurs et fichés, permettant de dégager des solutions qui, tout en intégrant les prescrits légaux, ménagent les intérêts légitimes des uns et des autres. On se doit de préciser que la saisine des autorités de contrôle peut être effectuée par toute personne ou association la représentant[183] et que les décisions « faisant grief » sont susceptibles de recours juridictionnel.

83. Pour que les autorités de contrôle puissent remplir leurs missions de manière efficace, la directive impose de leur reconnaître des pouvoirs d'investigation. Définis en termes larges, ces pouvoirs ont pour objet de permettre aux autorités d'accéder aux données traitées et de recueillir toutes informations nécessaires à leur tâche[184]. En outre, des possibilités spécifiques d'intervention doivent leur être octroyées, telles l'émission d'avis préalablement à la mise en œuvre des traitements[185], la publication appropriée de ces avis, la possibilité soit d'ordonner le verrouillage, l'effacement ou la destruction de données, soit d'interdire un traitement (à titre définitif ou temporaire) ou d'adresser un avertissement ou une admonestation au responsable du traitement, soit enfin de saisir les parlementaires nationaux ou d'autres institutions politiques.

179 Le 62e considérant qualifie l'institution d'autorités de contrôle exerçant leurs fonctions en toute indépendance d'élément « essentiel » pour la protection des personnes.

180 De manière paradoxale, lorsque l'État décide de la mise en place d'importants traitements de données à caractère personnel, l'intervention d'autorités de contrôle peut conduire à renforcer le pouvoir de celui-ci, lorsque celles-ci avalisent son intervention, garantissant par leur « indépendance » que la protection des droits et libertés des citoyens est suffisamment prise en compte.

181 La directive ne prévoit pas explicitement que les avis revêtent un caractère obligatoire. La formulation de article 28, § 2, de la directive envisage la consultation des autorités de contrôle « lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel ». Tout dépendra donc de l'appréciation des instances réglementaires quant à l'impact des mesures envisagées sur la protection des droits et libertés des personnes.

182 L'obligation d'établir un rapport d'activité participe clairement à cette mission d'information du public (cf. infra). D'autres moyens peuvent cependant être envisagés, comme les communiqués de presse, les brochures d'information, etc.

183 En vertu de l'article 28, § 4, la personne concernée doit être informée des suites réservées à sa demande.

184 Les législations en vigueur dans les États membres accordent généralement de tels pouvoirs aux autorités actuellement en place. On peut citer à titre d'exemple, la loi française du 6 janvier 1978 qui reconnaît, en ses articles 11 et 21, à la Commission nationale de l'informatique et des libertés le pouvoir de se faire communiquer tous renseignements et documents utiles à sa mission, mais exclut tout pouvoir contraignant tel que perquisition ou saisie. La Convention n° 108 ne prévoit, quant à elle, rien de comparable.

La directive reconnaît aux autorités le pouvoir d'ester en justice ou de porter les violations constatées à la connaissance du pouvoir judiciaire. Jusqu'à présent, les États membres privilégiaient fréquemment la deuxième solution[186]. Les deux possibilités sont à présent explicitement prévues.

84. On doit encore signaler que lorsque des dispositions nationales sont adoptées en application de l'article 13 de la directive[187], chaque autorité de contrôle peut être saisie par toute personne d'une demande de vérification de la licéité d'un traitement. Si cette procédure s'apparente en partie à ce que certains pays, comme la Belgique et la France, ont mis en place pour des traitements particuliers, chargeant l'autorité de contrôle de l'exercice du droit d'accès[188], elle s'étend plus largement à un examen général de la licéité des traitements pour lesquels des mesures législatives ont limité la portée de certaines obligations.

Par ailleurs, les autorités de contrôle sont tenues de publier un rapport d'activité. On insistera sur l'importance de la publication de tels rapports. C'est en effet par cette voie que les organes rendent compte de l'accomplissement de leurs missions devant les parlements qui les ont institués, mais surtout, cette transparence permet aux acteurs de la vie économique et politique d'avoir connaissance des positions des autorités de contrôle et d'adapter leur comportement en conséquence.

La directive prévoit également que les autorités de contrôle coopèrent entre elles[189]. En termes d'expertise développée par chacune d'entre elles, cette collaboration relève du bon sens dans la mesure où les réglementations nationales trouveront un fondement commun dans la directive et dès lors qu'il est indispensable d'éviter que les responsables de traitement ne soient tentés de faire usage de manière abusive de la liberté des flux de données à caractère personnel reconnue par la directive. En outre, dans la mesure où les problèmes se posent fréquemment de manière similaire dans chacun des États membres, autant bénéficier de l'expérience de l'étranger...

85. En définitive, l'impact des autorités de contrôle au sein des États membres qui les instituent, dépendra de leurs réelles possibilités d'action, à savoir le fait de disposer d'incitants ou de sanctions suffisamment forts pour que leurs prises de position soient suivies d'effets. L'impact de l'action de ces autorités est également étroitement lié à la qualité de leurs décisions et au fait que ces dernières sont adoptées en connaissance de cause, et plus particulièrement sur la base de discussions approfondies avec les intéressés. On peut cependant s'interroger sur l'effectivité de leurs moyens d'intervention face

185 Cf. supra, la notification. Voy. à titre de comparaison, l'article 1.3 de la recommandation R(87) 15 sur les données de police (précitée) qui suggère que l'avis de l'autorité de contrôle soit recueilli préalablement à la mise en œuvre d'un traitement automatisé.

186 Il en est ainsi pour la loi française de 1978 qui ne reconnaît à la CNIL que le pouvoir de dénoncer une infraction au parquet qui, quant à lui, reste libre de classer ou non l'affaire.

187 Cf. supra.

188 Cette procédure est connue en France sous le vocable « accès indirect ». Elle concerne par exemple l'accès aux traitements liés à la sécurité de l'État, aux services de renseignements, à la police.

189 De la même manière, l'article 13, a, de la Convention n° 108 prévoit une collaboration entre autorités, par la fourniture d'informations tant sur les réglementations et pratiques que sur des éléments de fait concernant les traitements de données effectués sur leur territoire.

à des délocalisations de traitements dans les lieux non soumis à leur compétence et en présence de technologies de traitement de l'information évoluant sans cesse[190].

II. Le contrôle au niveau communautaire

1. Le groupe européen de protection

86. La directive instaure, en son article 29, un groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel[191].

Divers groupes à vocation internationale s'occupaient déjà de questions de protection des données. Ainsi, la Convention du Conseil de l'Europe avait institué un comité consultatif chargé d'améliorer la Convention, de l'interpréter ou de la réviser[192]. Par ailleurs, la conférence des commissaires européens avait spontanément vu le jour à l'initiative des autorités de contrôle européennes existantes, en réaction précisément au projet de directive[193].

87. Le groupe institué par la directive est dénué de pouvoir décisionnel. Il est composé d'un représentant de l'autorité ou des autorités de contrôle nationales désigné par chaque État membre, mais comprend, en outre, un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et un représentant de la Commission européenne[194].

Il a pour mission de contribuer à la mise en œuvre homogène des lois nationales, de donner un avis à la Commission sur le niveau de protection dans la Communauté et les pays tiers[195], de conseiller la Commission pour amender la directive et de donner un avis sur les codes de conduite communautaires. Le groupe peut également émettre des recommandations sur toute question concernant la protection des personnes et établit un rapport annuel publié[196].

88. La reconnaissance par la directive de l'intérêt de prévoir un forum de discussions entre commissaires européens est une démarche positive. Il est en effet important de donner une portée concrète à l'article 28, § 6, et d'institutionnaliser la coopération entre les autorités de contrôle. Mais ne devrait-on pas franchir une étape supplémentaire et octroyer à ce groupe des pouvoirs effectifs d'intervention ?

Par ailleurs, hors la directive et le droit communautaire, différents textes règlent l'échange de données à caractère personnel dans le contexte du troisième pilier du traité de Maastricht[197] et ont institué en matière policière, douanière et judiciaire, chacune

190 A l'origine, l'instauration d'autorités de contrôle répondait précisément au besoin d'apporter des réponses rapides, éclairées et adaptées à des problèmes que les pouvoirs traditionnels semblaient peu à même d'appréhender. Dans ce contexte, la recherche d'une médiation faisait figure d'approche privilégiée.

191 Ce groupe qui se réunit au rythme de quatre réunions par an, fonctionne de manière effective depuis le mois de janvier 1996.

192 Articles 14, 19 et 20 de la Convention n° 108.

193 La conférence des commissaires européens a vu le jour en 1994. Par ailleurs, depuis près de vingt ans, existe la conférence internationale des commissaires à la protection des données au sein de laquelle sont représentés une trentaine de pays.

194 Le comité consultatif se compose, pour sa part, de représentants désignés par les États signataires eux-mêmes (voy. article 18, § 2, de la Convention n° 108).

195 L'intervention du groupe doit être envisagée comme l'un des divers mécanismes tendant à garantir une approche commune en matière de flux à destination de pays tiers.

196 En vertu de l'article 30, § 5, la Commission doit informer le groupes des suites réservées à ses avis et recommandations et rédiger à cet effet un rapport publié qui devrait être transmis au Parlement et au Conseil.

197 Conventions ou futures conventions.

pour la matière qui la concerne, une autorité de contrôle (autorité de contrôle commune Europol, autorité de contrôle Eurodac, autorité de contrôle commune S.I.D.). Le paradoxe de cette situation provient de ce que chacune des instances n'est compétente que pour les données visées par la convention qui l'institue. Or, les services utilisateurs font usage de l'ensemble des données rendues disponibles par les différentes conventions. En outre, on peut craindre que les autorités sectorielles enfoncées dans leurs problèmes spécifiques, ne perdent de vue les questions plus générales et la nécessité d'une approche globale de celles-ci. A terme, ne serait-il pas dès lors préférable qu'une seule et même autorité soit chargée de contrôler l'ensemble des données échangées dans le cadre du troisième pilier du traité de Maastricht?

2. Le contrôle au niveau des institutions communautaires

89. Il serait utile que soit instaurée une autorité de contrôle chargée de veiller au respect des règles de protection des données par les institutions communautaires. Une résolution du Parlement européen a été adoptée en ce sens[198]. La directive n'étant pas applicable aux autorités européennes, celles-ci ne sont pas tenues de mettre en place une telle instance[199]. Sa mise en place nous paraît cependant fondamentale en vue de garantir la protection des données à caractère personnel lors des échanges d'informations entre les États membres et les institutions communautaires. Le projet de traité d'Amsterdam, adopté lors du Conseil européen des 16 et 17 juin 1997, prévoit d'ailleurs de combler ces lacunes par l'insertion d'un nouvel article 213B dans le traité instituant la communauté européenne. En vertu de cette disposition, la directive sera applicable aux institution communautaires à partir du 1er janvier 1999, tandis qu'un organe indépendant de contrôle aura été institué avant cette date, comme, bien entendu, que le traité d'Amsterdam entre en vigueur.

3. L'exécution des mesures communautaires

90. Enfin, l'article 31 institue un groupe composé des représentants des États membres et présidé par le représentant de la Commission. Son rôle consiste à assister la Commission dans l'exécution de la directive, en particulier en ce qui concerne le transfert de données vers les pays tiers[200]. La composition de ce groupe, à savoir les représentants des États membres, indique à suffisance l'enjeu éminemment politique de cette question. Ce groupe peut dans une certaine mesure être comparé au comité d'experts du Conseil de l'Europe qui élabore les recommandations. Toutefois, son pouvoir semble s'apparenter davantage à celui d'un organe consultatif selon la procédure fixée par la comitologie[201].

H. Recours, responsabilités et sanctions

91. Deux types de recours sont prévus en cas de violation des lois nationales prises en conformité avec la directive.

198 Le point 42 de la résolution du Parlement européen sur le bilan 1996 et le programme 1997, votée le 11 décembre 1996, demande un système de supervision indépendant pour la protection des données personnelles par les institutions et organes de l'Union, ainsi qu'une réglementation générale contenant les conditions minimales et les principes fondamentaux de l'accès au public des documents européens.

199 La directive fait cependant indirectement allusion à la création d'une telle autorité lorsqu'elle inclut dans la composition du groupe institué en vertu de son article 29, § 2, un représentant « de l'autorité ou des autorités crées pour les institutions et organismes communautaires ».

200 Voy. le considérant 66.

201 Décision du Conseil du 13 juillet 1987 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission, J.O.C.E., 1987, n° L 197/34.

L'article 22 prévoit la possibilité pour les États membres d'organiser un recours administratif devant les autorités de contrôle et cela, préalablement à la saisine de l'autorité judiciaire.

Les États membres ont cependant l'obligation d'offrir à la personne concernée par les données un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. La nature du recours et ses règles propres tombent pour le reste dans la compétence souveraine des États membres.

92. L'article 23 proclame, dans la suite de l'existence du recours, le droit de la personne concernée d'obtenir du responsable du traitement réparation des dommages subis du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la directive. Le second alinéa de cette disposition permet aux États membres d'exonérer le responsable du traitement s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Ce texte pourrait donner lieu à des difficultés d'interprétation. Il n'est en effet pas aisé de déterminer s'il introduit un système de responsabilité classique fondé sur la preuve d'une faute, d'un dommage et du lien causal ou si cette responsabilité est présumée de la simple constatation du dommage naissant d'un traitement illicite ou d'une action incompatible avec les règles nationales. L'absence de référence à la notion de faute – un traitement illicite et, *a fortiori,* une action « incompatible » avec les dispositions nationales n'impliquent pas forcément une faute dans le chef du responsable du traitement[202] –, la possibilité d'exonération concernant les seules causes étrangères[203] et l'évolution même de la disposition dans ses différentes versions[204] pourraient fonder l'idée de la mise en place d'une véritable présomption de responsabilité. Par contre, l'absence d'indications claires et précises en ce sens dans les différents documents officiels publiés, la référence pour certaines obligations au critère de diligence[205] et le considérant n° 55[206] inciteraient à penser que les États membres restent libres d'appliquer leurs règles de droit commun de la responsabilité en la matière.

93. Enfin, l'article 24 impose aux États membres de prévoir des sanctions applicables en cas de violation des dispositions nationales prises en application de la directive. La nature de ces sanctions est laissée à leur libre appréciation, même si le considérant 55 rappelle que celles-ci doivent être appliquées à toute personne, tant de droit privé que de droit public, qui ne respecte pas les dispositions visées.

202 Un traitement contenant des données inexactes est assurément illicite, mais n'implique pas forcément une faute du responsable du traitement, notamment si les États nationaux y voient le lieu d'une obligation de diligence et de prudence.

203 Le considérant n° 55 vise explicitement la faute de la victime et le cas de la force majeure.

204 Dans ses deux premières versions, la disposition ne permettait l'exonération du responsable du traitement que dans le seul cas où il parvenait à démontrer qu'il avait pris les mesures de sécurité appropriées pour respecter les exigences de l'actuel article 17 (sécurité). Ce faisant, l'alinéa 2 de la disposition commentée ne venait que préciser une exonération parfaitement logique dans un système de responsabilité basé sur la faute. Entre-temps, le Parlement européen avait proposé de faire disparaître cette exonération en la remplaçant par un système de responsabilité plus objective : « Le responsable des données indemnise la personne lésée pour tout dommage ou préjudice résultant d'une enregistrement de ses données personnelles incompatible avec les dispositions de la présente directive » (avis du Parlement du 11 mars 1992, J.O.C.E. n° C 94 du 13 avril 1992, p. 192). La dernière version de l'alinéa 2 de l'article 23 apparaît dès lors comme une voie médiane entre la version de la Commission et celle avancée par le Parlement européen.

205 Voy. l'article 2, d, (« toutes les mesures raisonnables doivent être prises pour que les données inexactes (. . .) soient effacées ou rectifiées ») ; l'article 17 relatif aux règles de sécurité paraît également viser une obligation de diligence.

206 Ce considérant présente l'existence d'un recours juridictionnel et de sanctions comme un remède au non-respect par le responsable du traitement de la loi nationale prise en application de la directive, ce qui semble revenir à viser la faute du responsable du traitement.

I. Conclusion

94. En définitive, la *ratio legis* de la directive du 24 octobre 1995 pourrait se résumer en peu de mots : laisser circuler librement les données sous protection rapprochée. En effet, pour permettre une libre circulation des données à caractère personnel dans le cadre du marché intérieur, il fallait veiller à une harmonisation des législations nationales de protection des données au regard des droits et libertés des individus. Il s'agissait premièrement de rapprocher entre elles des normes nationales en prévoyant un régime commun de protection. Mais il s'indiquait tout autant d'amplifier la protection des données à caractère personnel pour « rapprocher » l'individu de la maîtrise de son image informationnelle, appelée à voyager nettement plus vite que lui depuis les développements de la société de l'information.

95. L'œuvre normative des institutions de la Communauté européenne s'est avant tout alimentée du terreau fourni depuis janvier 1981 par le Conseil de l'Europe. La Convention n° 108 adoptée sous l'égide de ce dernier avait effectivement inspiré des législations de protection des données dans la plupart des États membres. Nonobstant, la directive entendait aller au-delà des dispositions de la Convention n° 108 pour hausser le niveau de protection garanti par ce biais initial. Dans cette optique, elle précise les principes généraux établis par ladite Convention, comme la récurrente comparaison des deux textes opérée ci-avant s'est employée à le démontrer. *Ipso facto,* la directive perd un des atouts de la Convention n° 108 dont le caractère général permet la prise en compte des innovations technologiques successives. L'adaptabilité de la directive au progrès technologique, tel celui que constitue l'incontournable phénomène d'Internet, semble d'ailleurs dès à présent susciter des problèmes que seule une transposition évolutive des dispositions de la directive par les États membres pourrait résoudre[207].

96. Enfin, la directive entend régler le sort des données à caractère personnel transmises aux États tiers. Ces données doivent bénéficier d'une protection adéquate au-delà des frontières de l'Union européenne pour franchir celles-ci. La protection adéquate pourrait faire de la directive, à terme, une référence normative dont les États tiers s'inspireraient pour la protection des données à caractère personnel qui ne seraient pas directement issues de la Communauté européenne. Cet effet d'engrenage (*spill over*) externe ne serait pas le moindre des mérites de la directive, du moins si l'on considère qu'il en va, *in fine,* des droits et libertés de tout individu, quel qu'il soit, où qu'il se trouve. . .

207 Voy. *M. H. Boulanger, C. de Terwangne,* op. cit.